



Payment Card Industry (PCI) Data Security Standard

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

June 2018

4

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:	SecuTix SA - ePaymentcenter	DBA (doing business as):	n/a
Contact Name:	Marco Ferro	Title:	PCI Compliance Officer
Telephone:	+41 (21) 6132111	E-mail:	marco.ferro@elca.ch
Business Address:	Place de'l Europe 8	City:	Lausanne
State/Province:	---	Country:	Switzerland
URL:	www.elca.com	Zip:	1001

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

Company Name:	Adsigno AG		
Lead QSA Contact Name:	Albrecht Duerr	Title:	Head of Audit Division PCI DSS
Telephone:	+49 176 1235 09 03	E-mail:	albrecht.duerr@adsigo.com
Business Address:	Koenigsallee 43	City:	Ludwigsburg
State/Province:	---	Country:	Germany
URL:	www.adsigo.com	Zip:	71638

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: ePC environment

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):

Account Management

Back-Office Services

Billing Management

Clearing and Settlement

Network Provider

Others (specify):

Fraud and Chargeback

Issuer Processing

Loyalty Programs

Merchant Services

Payment Gateway/Switch

Prepaid Services

Records Management

Tax/Government Payments

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: n/a

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
- Back-Office Services
- Billing Management
- Clearing and Settlement
- Network Provider
- Others (specify):

- Fraud and Chargeback
- Issuer Processing
- Loyalty Programs
- Merchant Services

- Payment Gateway/Switch
- Prepaid Services
- Records Management
- Tax/Government Payments

Provide a brief explanation why any checked services were not included in the assessment: n/a

Part 2b. Description of Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Cardholder data (PAN, name, expiry, CVV) for ecommerce ticket purchases is received from web shops by the payment gateway ePC and forwarded to payment processors and acquirers. Cardholder data is stored in the database of ePC until authorization and deleted afterwards

Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.

The entity under review performs cardholder data processing and switching for ecommerce merchants.

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):
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Head Office	1	Lausanne, Switzerland



Data Center

1

Lausanne, Switzerland

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)
ePC	7.9.5	Secutix	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	n/a
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> 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.

Payment application environment including the payment application (ePC) network infrastructure (firewall, switches), critical system components (application server, database server), supporting infrastructure (time server, access control server) as well as system components with security functionality (IDS, log server)

Does your business use network segmentation to affect the scope of your PCI DSS environment?

Yes No

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



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: n/a

QIR Individual Name: n/a

Description of services provided by QIR: n/a

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:
Logitours (NTT Europe Ltd.)	authorization

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: ePC environment

PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach <small>(Required for all "Partial" and "None" responses. Identify which sub-requirements were not tested and the reason.)</small>
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>1.2.2 n/a: Routers are not in scope of this assessment. This was verified by inspection of data flows and was confirmed during the network interview by interview.</p> <p>1.2.3 n/a: The company does not use wireless networks in the scope of PCI DSS. This was verified by inspection of data flows and was confirmed during the network interview.</p>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	---
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>3.2.1, 3.2.3: n/a: The company does not process card present data</p> <p>3.5 x: Keys are managed by the application and are never exposed to individuals.</p>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1: n/a: The company does not use wireless networks in the scope of PCI DSS. This was verified by inspection of data flows and was confirmed during the network interview
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	---
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.5.2 n/a: n/a - Managed runtime environment (JAVA) which results in that the payment application is not effected by buffer overflow vulnerabilities.



Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	---
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>8.1.5: n/a - Interview yield that no vendor has access to the cardholder data environment. Review of the access control lists confirmed this.</p> <p>8.5.1: n/a: The company has no access to customer environments.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.1.2: n/a: n/a - Interview and inspections showed that public accessible network jacks do not exist.</p> <p>9.5.1 - 9.7.1 n/a: Removable electronic media containing cardholder data does not exist.</p> <p>9.8.1 n/a: Interview confirmed that hard-copy media materials are not existing. Location review confirmed that no hard-copy media is existing.</p> <p>9.8.2 n/a: Interviews confirmed that no hard disk have been replaced or temporary stored during the past 12 months.</p> <p>9.9.x: n/a: Inspection of the business processes showed that the company under review is not a merchant. It does not operate POS devices at the point of sales.</p>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	---
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>11.1.1: n/a - Compared the network diagram with the firewall ruleset and interviewed Int-1 who confirmed, that no wireless infrastructure exists within the cardholder data environment.</p> <p>11.2.2.a: n/a - Review of change tickets confirmed that no significant changes occurred during the past 12 months.</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9: n/a: Vendors do not have access to the company's network remotely. Review of the firewall rule set and the remote access settings including review of the access control list confirmed this.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	n/a: The company does not act as a shared hosting provider
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	n/a: The company does not use early TLS or SSL connections in the scope of PCI DSS

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: January 30, 2019-

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

5

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated January 30, 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*):

- Compliant:** All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; thereby SecuTix SA - ePaymentcenter 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

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 3.2.1, 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 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 data¹, CAV2, CVC2, CID, or CVV2 data², or PIN data³ 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 TÜV Süd

Part 3b. Service Provider Attestation

	
Signature of Service Provider Executive Officer ↑	Date: 30/01/2019
Service Provider Executive Officer Name:	Title:
SEVERIN VOISIN	Head of Business SSO

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

If a QSA was involved or assisted with this assessment, describe the role performed: Assessment and preparation of the compliance documentation.

	Date: January 30, 2019
Signature of Duly Authorized Officer of QSA Company ↑	QSA Company: Adsigno AG
Duly Authorized Officer Name: Albrecht Duerr	

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: n/a

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.

5

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

