



Payment Card Industry (PCI) Data Security Standard

Sertifi, Inc.

October 23, 2023

Attestation of Compliance for Onsite Assessments – Service Providers

Version 3.2.1

Revision 2

September 2022

Document Changes

Date	Version	Description
September 2022	3.2.1 Revision 2	Updated to reflect the inclusion of UnionPay as a Participating Payment Brand.

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:	Sertifi, Inc.		DBA (doing business as):	Not Applicable		
Contact Name:	Obafemi Shyllon		Title:	Cloud Cyber Security Specialist		
Telephone:	(866) 983-8877		E-mail:	pci@sertifi.com		
Business Address:	222 W Merchandise Mart Plaza, Suite 2300		City:	Chicago		
State/Province:	Illinois	Country:	USA		Zip:	60654
URL:	www.sertifi.com					

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

Company Name:	SecurityMetrics, Inc.				
Lead QSA Contact Name:	Thomas McCrory	Title:	Principal Security Analyst		
Telephone:	(801) 705-5664	E-mail:	aoc@securitymetrics.com		
Business Address:	1275 West 1600 North	City:	Orem		
State/Province:	Utah	Country:	USA	Zip:	84057
URL:	www.securitymetrics.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: Sertifi Agreement Platform

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

☐ 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: 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.

When a payment request is made in the Sertifi Agreement Platform, the cardholder will receive an email with a link to a payment page. The payment pages (apps.sertifi.net, www.sertifi.com, or www.sertifi.net) are served from web servers located at the Digital Realty data center in Elk Grove, Illinois. Within each payment page is an iFrame, which performs a transparent redirect to a web form served by Azure App Services located behind an Azure application gateway. Cardholder data entered into the web form may be sent to a third-party (TokenEX) for storage and tokenization or directly to a payment gateway for authorization. A token is retained for future transactions. All transmissions occur using HTTPS secured with at least TLS1.2.

Sertifi does not store cardholder data.

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

The Sertifi Agreement Platform processes and transmits cardholder data as part of the authorization service.

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	<i>Boston, MA, USA</i>
Corporate Office	1	Chicago, IL, USA
Microsoft Azure Data Centers (IaaS)	1	Redmond, WA, USA
Data Center	1	Elk Grove, IL, USA

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)
Not Applicable			<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.*

- All connections into and out of the in-scope Virtual Private Cloud instances in the Microsoft Azure environment
- All connections into and out of the in-scope systems at the Elk Grove, Illinois data center
- People, processes, and technologies used to support secure transmission to and from in-scope instances within the Microsoft Azure environment
- Manual and automated processes such as monitoring, patching, and responding to alerts performed by personnel located at the Chicago, Illinois offices, as applicable
- Secure software development

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:
Microsoft Azure	Infrastructure-as-a-Service (IaaS)
Digital Realty Trust, L.P.	Co-location
TokenEX, Inc.	Tokenization, Storage
Braintree (PayPal)	Payment Gateway/Transaction Processing
Merchant Link LLC	Payment Gateway/Transaction Processing
Shift4 Payments LLC	Payment Gateway/Transaction Processing
Elavon, Inc.	Payment Gateway/Transaction Processing
Stripe, Inc.	Payment Gateway/Transaction Processing
FreedomPay, Inc.	Payment Gateway/Transaction Processing
CardConnect, LLC	Payment Gateway/Transaction Processing
Datatrans AG/PCI Proxy	Payment Gateway/Transaction Processing
CyberSource/Authorize.Net	Payment Gateway/Transaction Processing
Zuora, Inc.	Payment Gateway/Transaction Processing
Planet Payment	Payment Gateway/Transaction Processing

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:		Sertifi Agreement 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:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1.2.2: N/A – No routers are in use. 1.3.6: N/A – No systems in the Sertifi environment store cardholder data.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2.1.1: N/A – No wireless technologies are connected to the Sertifi cardholder data environment. 2.2.3: N/A – No insecure services, daemons, or protocols are in use. 2.6: N/A – Sertifi is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3.1: N/A – No systems in the Sertifi environment store cardholder data. 3.4.1: N/A – Disk encryption is not used. 3.5 - 3.6.8: N/A – No systems in the Sertifi cardholder data environment store cardholder data.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	4.1.1: N/A – No wireless technologies are connected to the Sertifi CDE.
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	6.4.6: N/A – No significant changes in the previous year. 6.5.3: N/A – No systems or applications in the Sertifi environment store cardholder data.

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 – No third-party user accounts are present in the Sertifi cardholder data environment.</p> <p>8.5.1: N/A – Sertifi does not remotely access customer premises.</p> <p>8.7: N/A – No systems in the Sertifi environment store cardholder data.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>9.5 - 9.8.2: N/A – No media containing cardholder data is present in the Sertifi cardholder data environment.</p> <p>9.9 - 9.9.3: N/A – Sertifi does not maintain any devices that capture cardholder data via direct physical interaction.</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 – No wireless technologies are in use.</p> <p>11.2.3: N/A – No significant changes have occurred in the previous year.</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	12.3.9: N/A – No third-party user accounts are present in the Sertifi cardholder data environment.
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A – Sertifi is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A – Sertifi does not maintain any devices that capture cardholder data via direct physical interaction.

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>October 23, 2023</i>	
Have compensating controls been used to meet any requirement in the ROC?	<input checked="" type="checkbox"/> Yes	<input 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 **October 23, 2023**.

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>Sertifi, Inc.</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>Sertifi, Inc.</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"> <thead> <tr> <th>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</i> , Version 3.2.1, 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 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. (<i>Not Applicable</i>)
<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, CVN2, CVV2, or CID 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>Tenable</i>)

Part 3b. Service Provider Attestation

Nick Demetralis

Signature of Service Provider Executive Officer ↑	Date: October 25, 2023
Service Provider Executive Officer Name: Nick Demetralis	Title: Director of IT Operations and Security

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

If a QSA was involved or assisted with this assessment, describe the role performed:	<i>The QSA, Thomas McCrory, assessed and validated all items described in the Report on Compliance, performed all interviews, and completed all report writing.</i>
--	---

Thomas McCrory

Signature of Duly Authorized Officer of QSA Company ↑	Date: October 25, 2023
Duly Authorized Officer Name: Thomas McCrory	QSA Company: SecurityMetrics, Inc.

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

