Payment Card Industry (PCI)
Software Security Framework

Secure Software Attestation of Validation

Version 1.2

April 2023

Document Changes

Date	Version	Description
March 2020	1.0	Initial release of the *PCI Secure Software Attestation of Validation* for *PCI Secure Software Requirements and Assessment Procedures* version 1.0.
April 2021	1.1	Updated AOV to align with updates to the *PCI Secure Software Requirements and Assessment Procedures* version 1.1 and the corresponding *PCI Secure Software Template for Report on Validation (ROV)*.
April 2023	1.2	Updated AOV to align with updates to the *PCI Secure Software Requirements and Assessment Procedures* version 1.2 and the corresponding *PCI Secure Software Template for Report on Validation (ROV)*.

Table of Contents

Secure Software Attestation of Validation

Instructions for Submission

This document, the *Payment Card Industry (PCI) Secure Software Attestation of Validation (AOV)*, must be completed as a declaration of the Payment Software's compliance with the *PCI Secure Software Requirements and Assessment Procedures* (Secure Software Standard). The completion of this document by the Payment Software Vendor for the sole purpose of Annual Revalidation does not require use of a Secure Software Assessor.

Capitalized terms that are used herein, but not defined, have the meanings ascribed to them in the then-current version of (or successor documents to) the *Payment Card Industry (PCI) Software Security Framework: Secure Software Program Guide* (Secure Software Program Guide), as from time to time amended and made available on the PCI Security Standards Council (PCI SSC) website at www.pcisecuritystandards.org.

The Secure Software Assessor (as defined in the *Payment Card Industry (PCI) Software Security Framework: Qualification Requirements for Assessors*) and/or the Payment Software Vendor must complete all applicable sections and submit this document with copies of all required validation documentation to PCI SSC per PCI SSC's instructions for report submission as described in the *Secure Software Program Guide*.

Note: *Parts 1 and 2 must be completed for all submissions.*

Part 1. Payment Software Vendor and Secure Software Assessor Information

Part 1a. Payment Software Vendor Information

Company Name:	PSR IT SOLUTIONS L.L.C.				
Contact Name:	Kirill Khaustov		Title:	CTO	
Telephone:	+971 508 963 259		E-mail:	kirill@psr.ae	
Business Address:	Office 3901-038, The One Tower, Al Thanyah First		City:	Dubai	
State/Province:	Dubai	Country:	UAE	Postal Code:	N/A
URL:	www.psr.ae				
Is the Vendor a Secure SLC Qualified Vendor?	☐ Yes ☒ No	If yes, PCI SSC Listing Reference Number:			

Part 1b. Secure Software Assessor Information

Company Name:	7Security GmbH				
Secure Software Assessor Name:	Yasen Georgiev		Title:	Information Security Expert	
Telephone:	+43 1 435 0000		E-mail:	y.georgiev@7sec.com	
Business Address:	Hiessgasse 12/3		City:	Vienna	
State/Province:	Vienna	Country:	Austria	Postal Code:	1030
URL:	www.7sec.com				

Part 2. Submission Type

Identify the type of submission and complete the indicated sections of this Attestation of Validation associated with the chosen submission type (select just one).
Refer to the *Secure Software Program Guide* for details about each submission type.

☒	**Full Assessment**	Complete Parts 3a, 3b, 4a, 4e, 5a and 5c
☐	**Annual Attestation**	Complete Parts 3a, 4b and 4e
☐	**Administrative Change (is a Secure SLC Qualified Vendor)**	Complete Parts 3a, 4c and 4e
☐	**Administrative Change (is not a Secure SLC Qualified Vendor)**	Complete Parts 3a, 4c, 4e, 5b and 5c
☐	**Low Impact (Delta) Change (is a Secure SLC Qualified Vendor)**	Complete Parts 3a, 4d and 4e
☐	**Low Impact (Delta) Change (is not a Secure SLC Qualified Vendor)**	Complete Parts 3a, 4d, 4e, 5b and 5c
☐	**High Impact Change (all Vendors)**	Complete Parts 3a, 4a, 4e, 5b and 5c

Part 3. Payment Software Information

Part 3a. Payment Software Identification

Payment Software Name: Pulsar POS
Payment Software Version Number: 1.1.0

Is the Payment Software already listed by PCI SSC?			☐ Yes *	☒ No
** If Yes:*	PCI SSC Listing #:	Not applicable	Expiry Date:	Not applicable
Is the Payment Software developed and managed under processes that are identified for the applicable Secure SLC Qualified Vendor on PCI SSC's list of Secure SLC Qualified Vendors on the PCI SSC website?			☐ Yes *	☒ No
** If Yes:*	PCI SSC Listing #:	Not applicable	Re-Assessment Date:	Not applicable

Part 3b. Payment Software Type

Primary function of the Payment Software (choose one):

☐ Automated Fuel Dispenser	☐ Payment Gateway/Switch	☐ POS Kiosk
☐ Card-Not-Present	☐ Payment Middleware	☐ POS Specialized
☐ Payment Back Office	☐ POS Admin	☐ POS Suite/General
☐ Payment Component	☒ POS Face-to-Face/POI	☐ Shopping Cart & Store Front

Part 4. Payment Software Vendor Attestation

PSR IT SOLUTIONS L.L.C. attests to and certifies the following regarding the Payment Software and version(s) thereof identified in Part 3 of this document as of *25 August 2026*. Complete one of Parts 4a, 4b, 4c or 4d; and 4e:

Part 4a. Confirmation of Validated Status: (each item to be confirmed)

☒	The Secure Software Assessor has been provided with all documentation and resources necessary to perform an accurate and complete assessment of the compliance of the Payment Software noted in Part 3 with the *Secure Software Standard*.
☒	We acknowledge our obligation to provide end-users of the Payment Software (either directly or indirectly through our resellers and integrators) with clear and thorough guidance on the secure implementation, configuration, and operation of the Payment Software.
☒	We have adopted and implemented documented Vulnerability Handling Procedures in accordance with our Vendor Release Agreement dated *(*19 September 2024*),* and confirm that we are and will remain in compliance with our Vulnerability Handling Procedures.

Part 4b. Annual Attestation

Based on the results noted in the *Payment Card Industry (PCI) Secure Software Report on Validation (ROV)* submitted to PCI SSC and dated *(date)*, *Payment Software Vendor Name* attests and certifies the following:

☐	No modifications have been made to the Payment Software **OR**
☐	Each modification made to the Payment Software has been submitted to and accepted by PCI SSC in accordance with the Secure Software Program Guide.
☐	The Validated Payment Software continues to meet all applicable requirements of the Secure Software Standard.
☐	All tested platforms, operating systems, and dependencies upon which the Validated Payment Software relies remain supported.

Part 4c. Administrative Changes

Based on internal change analysis and the completed *Secure Software Change Impact* documentation, *Payment Software Vendor Name* attests and certifies the following regarding the Payment Software and version(s) thereof identified in Part 3 of this document (each item to be confirmed):

☐	***Only Administrative Changes*** to the Validated Payment Software listing or how the Validated Payment Software is described in the List of Validated Payment Software have been made.
☐	All changes have been accurately recorded in the *Secure Software Change Impact* documentation provided with this attestation.
☐	We acknowledge our obligation to provide end-users of the Payment Software (either directly or indirectly through our resellers and integrators) with clear and thorough guidance on the secure implementation, configuration, and operation of the Payment Software.
☐	We have adopted and implemented documented Vulnerability Handling Procedures in accordance with our *Vendor Release Agreement* dated *(date)*, and confirm that we are and will remain in compliance with our Vulnerability Handling.

Part 4d. Change Analysis for Low Impact (Delta) Changes	
Based on the *Secure Software Change Impact* document, *Payment Software Vendor Name* attests and certifies the following regarding the Payment Software and version(s) identified in Part 3 of this document (each item to be confirmed):	
☐	Only ***Low Impact (Delta) Changes*** have been made to the Payment Software architecture, source code or components (does not trigger High-impact change criteria).
☐	All changes have been accurately recorded in the *Secure Software Change Impact* documentation provided with this attestation.
☐	Changes do not affect sensitive data, functions, or resources.
☐	We acknowledge our obligation to provide end-users of the Payment Software (either directly or indirectly through our resellers and integrators) with clear and thorough guidance on the secure implementation, configuration, and operation of the Payment Software.
☐	We have adopted and implemented documented Vulnerability Handling Procedures in accordance with our *Vendor Release Agreement* dated *(date)*, and confirm that we are and will remain in compliance with our Vulnerability Handling Procedures.

Part 4e. Payment Software Vendor Acknowledgment	
Подписант: Kirill Khaustov 18054F8597A44AD...	25 August 2026
Signature of Payment Software Vendor Executive Officer ↑	*Date* ↑
Kirill Khaustov	CTO
Payment Software Vendor Executive Officer Name ↑	*Title* ↑
PSR IT SOLUTIONS L.L.C.	
Payment Software Vendor Company Name↑	

Part 5. Secure Software Assessor Attestation

Based on the results noted in the *Payment Card Industry (PCI) Report on Validation (ROV)* dated *25 August 2026*, *7Security GmbH* attests and certifies the following regarding the Payment Software and version(s) identified in Part 3 of this document. Complete one of Parts 5a or 5b; and Part 5c:

Part 5a. Validated Status: (each item must be confirmed)

☒	**Validated**: All requirements in the ROV are marked "in place," thereby *Pulsar POS 1.1.0* has achieved validation with the *Secure Software Standard*.
☒	The ROV was completed according to *Secure Software Standard*, version *1.2.1*, in adherence with the instructions therein.
☒	All information within the above-referenced ROV and in this attestation represents the results of our assessment of the above PCI Secure Software Standard fairly in all material respects.

Part 5b. Secure Software Assessor Attestation

Based on the *Secure Software Change Impact* documentation provided by the Payment Software Vendor, the documentation supports the Vendor's assertion that **only changes** (check applicable field below) have been made to the Payment Software identified in Part 3 of this document resulting in:

☐	**Administrative Change** - no impact to compliance with the *Secure Software Standard* and/or security-related functions of the Payment Software.
☐	**Low Impact (Delta) Change** to compliance with the *Secure Software Standard* and/or security-related functions of the Payment Software.
☐	**High Impact Change** to compliance with the *Secure Software Standard* and/or security-related functions of the Payment Software.

Part 5c. Secure Software Assessor Company Acknowledgment

Signed by: Rozmari Asprilla 4F4F9F07682914D...	25 August 2026
Signature of Secure Software Assessor Company Executive Officer ↑	*Date* ↑
Rozmari Asprilla	Service Delivery Director
Secure Software Assessor Company Executive Officer Name ↑	*Title* ↑
7Security GmbH	
Secure Software Assessor Company Name ↑	

Part 6. PCI SSC Acceptance

PCI SSC does not assess or validate payment software for compliance with the *Secure Software Standard*. The signature below and subsequent listing of Payment Software on the List of Validated Payment Software signifies that the applicable Secure Software Assessor Company has determined that the Payment Software complies with the *Secure Software Standard*, that the Secure Software Assessor Company has submitted a corresponding ROV to PCI SSC, and that the ROV, as submitted to PCI SSC, has satisfied all applicable quality assurance review requirements as of the time of PCI SSC's review.

PCI Security Standards Council LLC	Digitally signed by PCI Security Standards Council LLC Date: 2026.09.01 16:54:43 -04'00'
Signature of PCI Security Standards Council ↑	*Date ↑*