



Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS)

Attestation of Validation

Version 3.2

May 2016

PA-DSS Attestation of Validation

Instructions for Submission

The Payment Application Qualified Security Assessor (PA-QSA) must complete this document as a declaration of the payment application's validation status with the Payment Application Data Security Standard (PA-DSS).

The PA-QSA and Payment Application Software Vendor should complete all applicable sections and submit this document along with copies of all required validation documentation to PCI SSC, per PCI SSC's instructions for report submission as described in the *PA-DSS Program Guide*.

Part 1. Payment Application Vendor and Qualified Security Assessor Information

Part 1a. Payment Application Vendor Information

Company Name:	Shift4 Payments LLC				
Contact Name:	Mike Niederhauser	Title:	GRC Analyst		
Telephone:	702.597.2480 x3551	E-mail:	mniederhauser@shift4.com		
Business Address:	2202 N. Irving St.	City:	Allentown		
State/Province:	PA	Country:	USA	Postal Code:	18109
URL:	www.shift4.com				

Part 1b. Payment Application Qualified Security Assessor (PA-QSA) Company Information

PA-QSA Company Name:	Dara Security				
Lead PA-QSA Name:	Barry Johnson	Title:	President/CEO		
Telephone:	775.622.5386	E-mail:	barryj@darasecurity.com		
Business Address:	10580 N. McCarran Blvd. #115-337	City:	Reno		
State/Province:	NV	Country:	USA	Postal Code:	89503
URL:	www.darasecurity.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 (check only one).

<input type="checkbox"/>	Full Validation	Complete Parts 3a, 3c, 4a, 4d, 5a, & 5c
<input checked="" type="checkbox"/>	Annual Revalidation	Complete Parts 3b, 3c, 4b, & 4d
<input type="checkbox"/>	Administrative Change	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
<input type="checkbox"/>	No Impact Change	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
<input type="checkbox"/>	Low Impact Change	Complete Parts 3a, 3b, 3c, 4c, 4d, 5b, & 5c
<input type="checkbox"/>	High-Impact Change	Complete Parts 3a, 3c, 4a, 4d, 5a, & 5c

Part 3. Payment Application Information

Part 3a. Payment Application Identification

Payment Application name(s) and version number(s) included in this PA-DSS review:

Application Name:	Version Number:
-------------------	-----------------

Required Dependencies:

- | | |
|--------------------------|---------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | The Payment Application was assessed and is validated to use wildcards as part of its versioning methodology. |
| <input type="checkbox"/> | The Payment Application does not use wildcards as part of its versioning methodology. |

Part 3b. Payment Application References

Reference Payment Application name and version number currently on the PCI SSC List of Validated Payment Applications:

Application Name: 4Go	Existing Version Number: 4.6
PCI SSC Reference Number: 16-06.00127.017	Required Dependencies: UTG 4.7
	Verifone Mx925/Mx915
	ID Tech SecuRED & SREDKey
	Ingenico IPP310, iPP320, iPP350
	Ingenico iSC250
	Ingenico iSC350
	Ingenico iSC Touch 480
	Ingenico iSMP
	Ingenico iCMP
	Ingenico IUP250
	Ingenico IUR250, IUR250P
	Ingenico iUC150B
	Ingenico iUC285
	Honeywell Captuvo SL22, SL42, or SL62
	ID Tech BTMAG, iMag Pro II, iMag Pro, SecureKey M100/M130, SecureMag, Shuttle, Spetrum Air, UniMag II, Xpress CM100
	Ingenico iWL252 or iWL258

Description of change, if applicable: None

Part 3c. Payment Application Functionality & Target Market

Payment Application Functionality (check only one):

<input type="checkbox"/> Automated Fuel Dispenser	<input type="checkbox"/> POS Kiosk	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Card-Not-Present	<input checked="" type="checkbox"/> POS Specialized	<input type="checkbox"/> Payment Middleware
<input type="checkbox"/> POS Admin	<input type="checkbox"/> POS Suite/General	<input type="checkbox"/> Payment Module
<input type="checkbox"/> POS Face-to-Face/POI	<input type="checkbox"/> Payment Back Office	<input type="checkbox"/> Shopping Cart & Store Front

Target Market for Payment Application (check all that apply):

<input type="checkbox"/> Retail	<input type="checkbox"/> Processors	<input type="checkbox"/> Gas/Oil
<input type="checkbox"/> e-Commerce	<input type="checkbox"/> Small/medium merchants	
<input checked="" type="checkbox"/> Others (please specify): All		

Part 4. Payment Application Vendor Attestation

Company asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 4d (*Complete one of Parts 4a, 4b, or 4c; and Part 4d*):

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

<input type="checkbox"/>	The PA-QSA has been provided with all documentation and resources necessary to reach an accurate assessment of the PA-DSS compliance status of the Payment Application and version noted in part 3a.
<input type="checkbox"/>	No track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data is stored subsequent to transaction authorization on ANY files or functionalities generated by the application.
<input type="checkbox"/>	We acknowledge our obligation to provide end-users of the Payment Application and version noted in part 3a (either directly or indirectly through their resellers and integrators) with a current copy of the validated payment application's <i>PA-DSS Implementation Guide</i> .
<input type="checkbox"/>	We have adopted and implemented documented Vulnerability Handling Procedures in accordance with Section 2(a)(i)(C) of the <i>Vendor Release Agreement</i> dated (<i>date</i>), and confirm we are and will remain in compliance with our Vulnerability Handling Procedures.

Part 4b. Annual Re-Validation Confirmation:

Based on the results noted in the PA-DSS ROV dated 23-Sept-2016, Company asserts the following as of the date noted in Part 4d:

Note: Part 4b is for the required Annual Attestation for listed payment applications, and should ONLY be completed if:

- No modifications have been made to the Payment Application covered by this AOV; OR
- A validated wildcard versioning methodology is being used and **only No Impact changes** have been made to the Payment Application covered by this AOV.

<input checked="" type="checkbox"/>	No modifications have been made to the Payment Application and version noted in part 3b
<input type="checkbox"/>	Payment Application and version noted in part 3b uses a validated wildcard versioning methodology and only No Impact changes have been made.
<input checked="" type="checkbox"/>	Vendor confirms that all tested platforms, operating systems, and dependencies upon which the application relies remain supported.
<input checked="" type="checkbox"/>	Vendor confirms that all methods of cryptography provided or used by the payment application meet PCI SSC's current definition of "strong cryptography."

Part 4c. Change Analysis for No Impact/Low Impact Changes

Based on internal change analysis and the Vendor Change Analysis documentation, Company asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 4d (check applicable fields):

<input type="checkbox"/>	Only changes resulting in No Impact or Low Impact to the PA-DSS requirements have been made to the "Parent" application noted above to create the new application also noted above.
<input type="checkbox"/>	All changes have been applied in a way that is consistent with our documented software-versioning methodology for this application in accordance with the <i>PA-DSS Program Guide</i> , and are accurately recorded in the Vendor Change Analysis provided to the PA-QSA noted in Part 1b.
<input type="checkbox"/>	All information contained within this attestation represents the results of the Vendor Change Analysis fairly in all material respects.

Part 4c. Change Analysis for No Impact/Low Impact Changes (continued)

- No track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data is stored subsequent to transaction authorization on ANY files or functionalities generated by the application.
- All methods of cryptography provided or used by the payment application meet PCI SSC's current definition of "strong cryptography."
- We acknowledge our obligation to provide end-users of the Payment Application and version noted in part 3b (either directly or indirectly through their resellers and integrators) with the updated copy of the validated payment application's *PA-DSS Implementation Guide*.

Part 4d. Payment Application Vendor Acknowledgment

<i>Scott Carcillo</i>	8/20/2020
<i>Signature of Application Vendor Executive Officer</i> ↑	<i>Date</i> ↑
Scott Carcillo	Chief Payments Officer
<i>Application Vendor Executive Officer Name</i> ↑	<i>Title</i> ↑
Shift4 Payments LLC	
<i>Application Vendor Company Represented</i> ↑	

Part 5. PA-QSA Attestation of PA-DSS Validation

Based on the results noted in the PA-DSS ROV dated (*date of ROV*), PA-QSA Company asserts the following validation status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 5c (*Complete one of Parts 5a or 5b; and Part 5c*):

Part 5a. Confirmation of Validated Status: (each item to be confirmed)

- | | |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Fully Validated: All requirements in the ROV are marked “in place,” thereby the Payment application and version noted in part 3a has achieved full validation with the Payment Application Data Security Standard. |
| <input type="checkbox"/> | The ROV was completed according to the PA-DSS, version (<i>insert version number</i>), in adherence with the instructions therein. |
| <input type="checkbox"/> | All information within the above-referenced ROV and in this attestation represents the results of the assessment fairly in all material respects. |
| <input type="checkbox"/> | No evidence of track data (magnetic-stripe data or equivalent data on the chip), CAV2, CVC2, CID, or CVV2 data, or PIN data storage exists after transaction authorization on ANY files or functionalities generated by the application during this PA-DSS Assessment. |

Part 5b. Low/No Impact Change – PA-QSA Impact Assessment

Based on the Vendor Change Analysis documentation provided by the Payment Application Vendor noted in Part 1a, (*Lead PA-QSA Name*) asserts the following status for the application(s) and version(s) identified in Part 3 of this document as of the date noted in Part 5c (check applicable fields). Based on our review of the Vendor Change Analysis documentation, we agree that the documentation supports the vendor’s assertion that **only Low Impact or No Impact changes** have been made to the application noted above, resulting in:

- | | |
|--------------------------|-----------------------------------------------------------------------------|
| <input type="checkbox"/> | No Impact to the PA-DSS Requirements and security-related functions |
| <input type="checkbox"/> | Low Impact to the PA-DSS Requirements and security-related functions |

Part 5c. PA-QSA Acknowledgment

Signature of Lead PA-QSA ↑	Date ↑
Lead PA-QSA Name ↑	Title ↑
PA-QSA Company Represented ↑	

Part 6. PCI SSC Acceptance

PCI SSC does not assess or validate payment applications for PA-DSS compliance. The signature below and subsequent listing of a payment application on the List of Validated Payment Applications signifies that the applicable PA-QSA has determined that the application complies with the PA-DSS, that the PA-QSA 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.

Signature of PCI Security Standards Council ↑	Date ↑