



**Attestation of Compliance – Service Providers
Payment Card Industry (PCI)
Data Security Standard**

**Attestation of Compliance for
Onsite Assessments – Service Providers**

Version 2.0

October 2010

Instructions for Submission

The Qualified Security Assessor (QSA) and Service Provider must complete this document as a declaration of the Service Provider's compliance status with the Payment Card Industry Data Security Standard (PCI DSS). Complete all applicable sections and submit to the requesting payment brand.

Part 1. Service Provider and Qualified Security Assessor Information

Service Provider Organization Information

Company Name:	Digital Payment Technologies	DBA(s):	
Contact Name:	Andrew Baxter	Title:	Director of IT
Telephone:	604.688.1959	E-mail:	andrew.baxter@digitalpaytech.com
Business Address:	4105 Grandview Highway	City:	Burnaby
State/Province:	BC	Country:	Canada
		Zip:	V5C 6B4
URL:	www.digitalpaytech.com		

Qualified Security Assessor Company Information

Company Name:	Payment Software Company, Inc (d/b/a PSC)		
Lead QSA Contact Name:	Thomas Arnold	Title:	Principal, PCI PA-QSA, Visa VSA
Telephone:	408 228 0961	E-mail:	tom@paysw.com
Business Address:	591 W Hamilton Ave, #200	City:	Campbell
State/Province:	CA	Country:	US
		Zip:	95008
URL:	www.paysw.com		

Part 2 PCI DSS Assessment Information

Part 2a. Services Provided that WERE INCLUDED in the Scope of the PCI DSS Assessment (check all that apply)

<input type="checkbox"/> Payment Processing-POS	<input type="checkbox"/> Tax/Government Payments	<input type="checkbox"/> Fraud and Chargeback Services
<input checked="" type="checkbox"/> Payment Processing-Internet	<input type="checkbox"/> Payment Processing – ATM	<input type="checkbox"/> Payment Processing – MOTO
<input type="checkbox"/> Issuer Processing	<input checked="" type="checkbox"/> Payment Gateway/Switch	<input type="checkbox"/> Clearing and Settlement
<input type="checkbox"/> Account Management	<input type="checkbox"/> 3-D Secure Hosting Provider	<input type="checkbox"/> Loyalty Programs
<input type="checkbox"/> Back Office Services	<input type="checkbox"/> Prepaid Services	<input type="checkbox"/> Merchant Services
<input type="checkbox"/> Hosting Provider – Web	<input type="checkbox"/> Managed Services	<input type="checkbox"/> Billing Management
<input type="checkbox"/> Network Provider/Transmitter	<input type="checkbox"/> Hosting Provider – Hardware	<input type="checkbox"/>
<input type="checkbox"/> Records Management	<input type="checkbox"/> Data Preparation	<input type="checkbox"/>
<input type="checkbox"/> Others (please specify):		

List facilities and locations included in PCI DSS review: Headquarters facility in Burnaby, BC, Canada; Data center in Vancouver, BC, Canada

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc.)? Yes No

Part 2c. Transaction Processing

How and in what capacity does your business store, process and/or transmit cardholder data? Client designs and manufactures multi-space parking meters for university, municipal and private parking lot operators. The parking meters connect securely in real time to Client's back end Enterprise Management System (EMS) service (a Internet payment gateway). EMS accepts transactions and switches them to upstream processors based on the individual parking lot operator's merchant account.

Please provide the following information regarding the Payment Applications your organization uses:

Payment Application in Use	Version Number	Last Validated according to PABP/PA-DSS
Bespoke	NA	Bespoke application

Part 3. PCI DSS Validation

Based on the results noted in the Report on Compliance ("ROC") dated 29 May 2013, Thomas Arnold, QSA asserts the following compliance status for the entity identified in Part 2 of this document as of 29 May 2013 (check one):

- Compliant:** All requirements in the ROC are marked "in place¹," and a passing scan has been completed by the PCI SSC Approved Scanning Vendor fee Secure ASV# 3709-01-03 thereby *Digital Payment Technologies* has demonstrated full compliance with the PCI DSS version 2.0.
- Non-Compliant:** Some requirements in the ROC are marked "not in place," resulting in an overall **NON-COMPLIANT** rating, or a passing scan has not been completed by a PCI SSC Approved Scanning Vendor, thereby (*Service Provider 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, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

QSA and Service Provider confirm:

- The ROC was completed according to the *PCI DSS Requirements and Security Assessment Procedures, Version 2.0*, and was completed according to the instructions therein.
- All information within the above-referenced ROC and in this attestation fairly represents the results of the assessment in all material respects.
- The Service Provider has read the PCI DSS and recognizes that they must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (that is, track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. QSA and Service Provider Acknowledgments



Signature of Service Provider Executive Officer ↑	Date: May 30, 2013
Service Provider Executive Officer Name: Chris Maghazic	Title: CTO

¹ "In place" results should include compensating controls reviewed by the QSA. If compensating controls are determined to sufficiently mitigate the risk associated with the requirement, the QSA should mark the requirement as "in place."

² 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 magnetic stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on the signature panel or face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



Signature of Lead QSA ↑ 	Date: 29 May 2013
Lead QSA Name: Thomas Arnold	Title: Principal, PCI PA-QSA

PSC

PAYMENTS :: SECURITY :: COMPLIANCE

Certificate of Completion to

Digital Payment Technologies

for their

2013 PCI Data Security Assessment

as a Service Provider

June 9, 2013

DIGITAL 
PAYMENT TECHNOLOGIES

PSC

PAYMENTS : SECURITY : COMPLIANCE

Certificate of Completion to

Digital Payment Technologies

for their

2012 PA-DSS Assessment

of their

LUKE II version 6.4

January 2, 2013

DIGITAL 
PAYMENT TECHNOLOGIES