Payment Card Industry (PCI)
Point-to-Point Encryption

P2PE Interim Assessment for Solutions:

Hardware/Hardware and Hardware/Hybrid

(For P2PE v1.x)

Version 1.0

August 2014

Document Changes

Date	Version	Description
August 2014	1.0	*Initial release of the P2PE Interim Assessment document*

Introduction

In order for a Validated P2PE Solution to remain on the List of Validated P2PE Solutions, it must undergo a new full P2PE Solution Assessment (resulting in Acceptance) every two years, and an "interim assessment" twelve months after each Acceptance.

Interim assessments (or "healthchecks") are required in order to provide additional confidence that between full assessments the:

- P2PE Solution continues to meet the requirements of the P2PE Standard
- P2PE Solution Provider's change management processes are operating effectively

All sections within this document must be completed. P2PE Interim Assessments must be submitted in a timely manner via the PCI SSC Portal with an updated Solution AOV in accordance with the *P2PE Program Guide*.

1.0 Contact Information, Report Date and P2PE Solution Details

1.1 Contact Information

Application Vendor contact information	
Company name:	
Company address:	
Company URL:	
Company contact name:	
Contact phone number:	
Contact e-mail address:	
P2PE Assessor Company contact information	
Company name:	
Company address:	
Company PCI credentials:	
P2PE Assessor contact information	
Assessor name:	
Assessor PCI credentials:	
Assessor phone number:	
Assessor e-mail address:	
P2PE Assessor Quality Assurance (QA) primary contact information	
QA primary contact name:	
QA primary contact phone number:	
QA primary contact e-mail address:	

1.2 Timeframe of Interim Assessment

Date of full P2PE listing:	
Dates of P2PE Interim Assessment:	

1.3 P2PE Version

P2PE Standard used for the assessment:	☐ Hardware/Hardware ☐ Hardware/Hybrid
Version of the P2PE Standard used for the assessment:	

1.4 Solution Overview

Solution Name:	
PCI SSC Reference #	

2.0   Devices and P2PE Applications in use for the P2PE Solution

2.1   List of PCI-approved POI Validated as Part of P2PE Solution (add rows as needed):

| Ref # | PTS Approval # | Make | Model | Hardware # | Firmware # | All Applications on POI | | Changed/Added since Last Full Assessment? | |
						Application Name	Version #	Yes	No
1								☐	☐
2								☐	☐
3								☐	☐

If any of the above has been answered "Yes" in the "Changed from Last Full Assessment" column, complete the following (add extra rows if needed):

| Ref # | Describe the Nature of the Change (Example: POI device addition, POI device removal) | Assessed in Designated Change? | | PCI SSC Reference # |
		Yes	No	
		☐	☐	
		☐	☐	
		☐	☐	

Note: Any outstanding Designated Changes should be submitted prior to submitting an Interim Assessment.

2.2 List of POI Applications Validated for Use with P2PE Solution: (add rows as needed)

Ref #	Application Name	Version #	Application Vendor	Application Has Access to Account Data?		Application on SSC List of Validated P2PE Applications?		SSC Listing Number (if applicable)	Changed/added since Last Full Assessment?	
				Yes	No	Yes	No		Yes	No
1				☐	☐	☐	☐		☐	☐
2				☐	☐	☐	☐		☐	☐
3				☐	☐	☐	☐		☐	☐
4				☐	☐	☐	☐		☐	☐
5				☐	☐	☐	☐		☐	☐

If any of the above has been answered "Yes" in the "Changed from Last Full Assessment" column, complete the following (add extra rows if needed):

Ref #	Describe the Nature of the Change (example: Application addition, Application removal)	Assessed in Designated Change?		PCI SSC Reference #
		Yes	No	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

Note: Any outstanding Designated Changes should be submitted prior to submitting an Interim Assessment.

3.0 Additional Verifications for Listed P2PE solutions

3.1 P2PE Decryption Environment (add rows as needed)

Complete each of the below to verify the following and identify changes to the solution since the last full P2PE solution assessment:		
1. Were any HSMs added, removed or changed?	☐ Yes	If yes, describe how the documentation was updated for the change for HSMs.
		If yes, describe how the Solution Provider implemented applicable P2PE controls:
	☐ No	
2. Were any third parties added, removed or changed (e.g., KIFs, CAs, POI installations, etc.)?	☐ Yes	If yes, describe how the documentation was updated for the change for third party support:
		If yes, describe how the Solution Provider implemented applicable P2PE controls:
	☐ No	
3. Has the decryption environment been verified as PCI DSS compliant within the last 12 months?	☐ Yes	
	☐ No	If no, provide an explanation: