Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI Security Standards Council bulletin on purchasing PCI approved devices

6 November 2018

As noted in the PCI PIN Transaction Security (PTS) Device Testing and Approval Program Guide, PTS POI vendors submit PTS devices for validation against the PTS POI Security Requirements. Devices that meet these requirements are then approved by PCI and listed on the PCI website ("Approved Devices"). The listing includes vendor name, device model name/number, hardware version, firmware version, and any other software impacting the POI Security Requirements. Vendors may make revisions to these devices, which are required to be assessed for security impact in 'Delta" reports. Subject to PTS Program requirements, any resulting changes in hardware or firmware versions are then added to the listing.

Under the PTS Program, all changes to an Approved Device's hardware or firmware are required to be assessed. Vendors may not unilaterally determine whether a change may or may not have security impact, but must instead submit the device changes for evaluation by a PCI PTS approved laboratory, who in turn must submit an evaluation report to PCI. Depending on the nature of the change(s) it may require changes in the hardware and/or firmware versions of the device, and if the changes are extensive enough, a full evaluation.

Vendors making modifications to Approved Devices must change the hardware and/or version number information. A modified device must undergo assessment by a PCI recognized laboratory and be approved by PCI to be listed as an Approved Device. Under PTS Program requirements, vendors are not permitted to make unevaluated changes that should impact the version number information on the approval listing and then represent the resulting changed product ("Substitute Product") as unchanged from the assessed and approved version. Vendors found to have intentionally engaged in this behavior are in breach of PTS Program requirements and may be subject to suspension, revocation or other conditions impacting PTS Program participation.

Background – Applying Device Listings

PCI requires that approved versions of Approved Devices must show the version numbers of hardware and firmware as shown in the PCI website list of Approved Devices. The hardware version number **must** be shown on a label attached to the device. The firmware (including PTS listed applications if applicable) version number, and optionally the hardware version number, **must** be shown on the display or printed during startup or on request.

The fields that make up the version numbers in the approval listings may consist of a combination of fixed and variable alphanumeric characters. A lower-case "x" is used by PCI to designate all variable fields. The "x" represents fields in the version numbers that the vendor can change at any time to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device color, language etc.

The "x" field(s) has/have been assessed by the laboratory and PCI SSC as to not impact the device's security requirements or the vendor's approval. To ensure that the payment security device has been approved, acquiring customers or their designated agents are strongly advised to purchase and deploy only payment security devices with the Hardware and Firmware #s whose fixed alphanumeric characters match exactly the Hardware and Firmware #s depicted on the PCI PTS Approved Device List.

In all cases the PCI website is considered the authoritative source for device status and should **always** be used to validate the approval status of a vendor's product.

For more information, please see the PCI PTS Device Testing and Approval Program Guide.

Action

To help ensure that entities deploying PTS devices deploy equipment that is the same as the PCI approved version, PCI recommends:

- Entities purchasing devices only purchase devices that are compliant with the requirements for labeling and displaying the hardware and firmware/application versions as stipulated above. Furthermore, the version numbers **must** be in accordance with the version numbers listed on the PCI website for that specific device model name/number. Devices not meeting the aforementioned **should not** be considered the PCI approved product version.
- Purchase orders for point-of-interaction PIN-acceptance devices **should** specify compliance to the applicable PCI Point of Interaction Security Requirements document. This should include specific vendor attestation as shown in the attached form that the PTS devices have been assessed and approved by PCI.

PTS Device Attestation

The PTS vendor must complete this document as a declaration of the device validation status with the PTS POI Security Requirements. The PTS vendor should complete all applicable sections and submit this document as requested by the purchaser.

Part 1. PTS Vendor					
Company name:					
Contact name:			Title:		
Telephone:			E-mail:		
Business address:			City:		
State/Province:		Country:		Postal code:	
URL:					

Part 2. Device Approval Information

For each applicable device, indicate hardware and firmware submission status as either:

A: No modifications have been made to the hardware or firmware versions as listed on the PCI website;

B: All hardware and firmware changes have been assessed by a PTS laboratory in a report submitted to PCI, including those hardware or firmware versions noted as using a validated wildcard versioning methodology.

PTS Approval Number	Model Name	Type A or B	Hardware Version	Firmware Version	Application Version (if applicable)
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			
		☐			

Part 3. PTS Vendor Acknowledgment

Signature of PTS Vendor Executive Officer ↗	*Date ↗*
PTS Vendor Executive Officer Name ↗	*Title ↗*

PTS Vendor Company Represented ↗