Payment Card Industry (PCI)

PIN Transaction Security (PTS)

Device Testing and Approval Program Guide

Version 2.1b

April 2024

`

Document Changes

Date	Version	Description
September 2010	1.0	Initial Release
October 2011	1.1	Added approval classes for encrypting card readers and non-PEDs.
July 2012	1.2	Added HSM v2 and clarifications for Fees, Approval Classes, and Expiry Dates.
September 2013	1.3	Updated for POI v4 and clarification for Integration, Open Protocols, SRED, device archival, determination of approval status, delta evaluations, submittal deadlines, fees, secure card readers and non-PEDs.
March 2014	1.4	Made changes in device sample requirements. Made additions to compromise notification process. Defined new device category—*Devices with Expired Approval.* Provided additional clarifications for Approval Class Features—PIN support, Key Management and Functions Provided. Updated definitions for non-PEDs and SCRs. Provided further explanations on the delta-evaluation process.
2015	1.5	Modified process for requesting change of business name/address/contact details via an Administrative Change Request Form submitted to the lab; change to invoice cycle; pro-rated invoices issued November 1 for all devices listed between May 2 – October 31. New guidance on licensing (re-branding) of another vendor's device.
2016	1.6	Updated for POI v5 and HSM v3. Testing timeframes restated. Added new HSM approval class information for Key Loading Devices and Remote Administration Platforms. Clarifications to product types for self-contained OEM products.
May 2017	1.7	Added requirement for security policy modification for administrative changes. Added text to call out where ISO PIN Block Format 4 is used for PIN encryption, specifically AES, and the method in which used—i.e., DUKPT, Fixed or Master/Session Key. Updated Appendix B for POI v5.
March 2018	1.8	Added SCRP approval class, including SCRP-only specifications for new approvals and expiry dates. Added requirement for annual Attestation of Validation regarding firmware changes (Section 3). Changes in side-channel testing. Added Appendix D: PTS Attestation of Validation. Errata.
June 2020	1.9	Migrated program-related Technical FAQs; updated Appendix D, "PTS Attestation of Validation"; added Appendix E, "PTS Device Attestation"; eliminated Vendor Questionnaire; errata.
May 2022	2.0	Added additional language from Technical FAQs. Updated for HSM v4.0 and POI v6.1. Updated for firmware expiry. Updated for required shipping information. Updated Approval Class, Approval Class Features and Expiry Dates sections. Updated Appendices B, C, and D.
December 2022	2.1	Updated firmware expiry, administrative changes, Appendices A and B.
February 2023	2.1a	Updated Expiry Date table.
April 2024	2.1b	Updated Approval Class Features and Expiry Dates sections.

Contents

1 Introduction

The following sections provide foundation and background information for this *PCI PIN Transaction Security Device Testing and Approval Program Guide* (the "Program Guide").

1.1 Related Publications

In addition to this Program Guide (describing the testing and approval process), the PCI Security Standards Council PIN Transaction Security (PTS) framework includes the following documents:

Note: *The documents below are routinely updated. The current versions should be referenced when using the Program Guide. Current standards generally are available at www.pcisecuritystandards.org.*

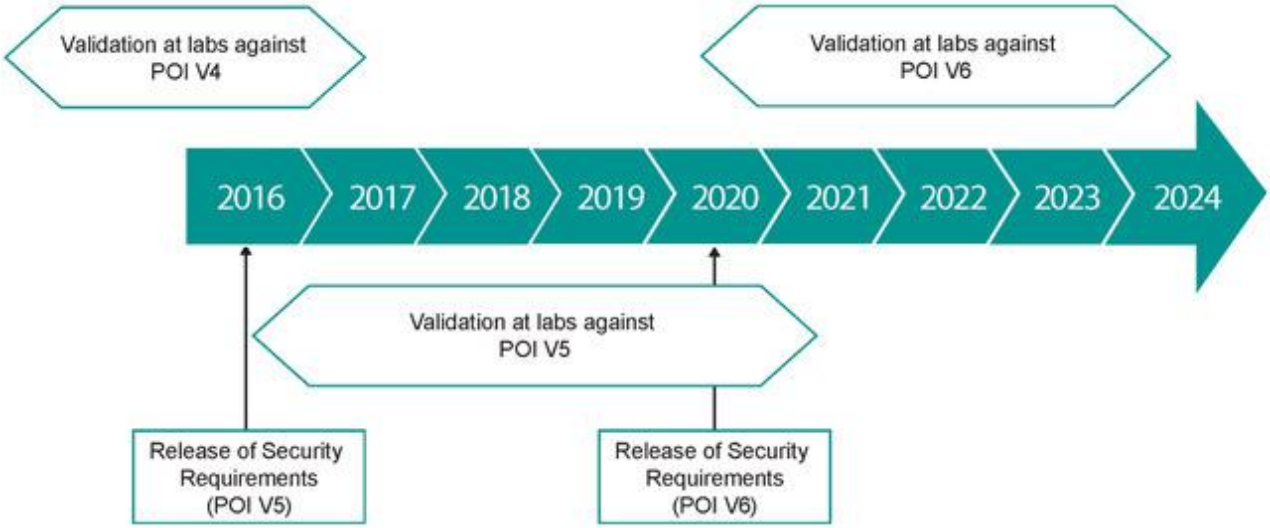
Document Name	Description
Security Requirements	
▪ *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements, v6.2* ▪ *PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Security Requirements, v4.0*	POI and HSM contain the physical and logical security device requirements as well as device management requirements for activity prior to initial key loading.
▪ *PCI PIN Security Requirements and Testing Procedures, v3.1*	PIN contains a complete set of requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.
FAQs	
▪ *PTS POI: Frequently Asked Questions*	General frequently asked questions.
▪ *PTS POI Security Requirements Technical FAQs for use with Version 6* ▪ *PTS PIN Security Requirements Technical FAQs for use with Version 3* ▪ *PTS HSM Security Requirements Technical FAQs for use with Version 4*	Provide additional and timely clarifications to the application of the above Security Requirements. The FAQs are an integral part of the Security Requirements and shall be fully considered during the evaluation process.

Document Name	Description
Derived Test Requirements	
▪ *PCI PIN Transaction Security (PTS) Point of Interaction (POI) Modular Derived Test Requirements, v6.2* ▪ *PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Modular Derived Test Requirements, v4.0*	Provide specific direction to vendors on methods the Laboratories may apply when testing against the Security Requirements.
PCI-Recognized Laboratories List	
▪ *Payment Card Industry (PCI)-Recognized Laboratories List*	List on the Website of test laboratories recognized and approved by PCI SSC as PTS Labs.
Vendor Release Agreement	
▪ *Payment Card Industry Vendor Release Agreement* (VRA)	Contains the terms and conditions that govern the exchange of information between vendors and PCI SSC and related PTS Program terms.
Approved Device List	
▪ *Approved PIN Transaction Security Devices*	List on the Website of PCI SSC-approved PIN Transaction Security Devices.

The documents described above are available in the "PTS" and "PIN" subsections of the "Document Library" section of the PCI SSC Website. Earlier versions of the documents are available in the Archived Documents section of the Website.

1.2 Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, PCI SSC regularly reviews, updates, and improves its Security Requirements used to evaluate POI devices and hardware security modules, collectively referred to as "payment security devices." PCI SSC periodically updates all corresponding PTS Security Requirements and associated test requirements (collectively, "Security Requirements"). The following diagram describes the life cycle of *PCI PTS POI Modular Security Requirements v5*, its predecessors, and successor v6.



PCI SSC reserves the right to change, amend, or withdraw Security Requirements at any time. If such a change is required, PCI SSC endeavors to work closely with vendors and other affected stakeholders to help reduce the impact of any changes.

1.3 About This Document

The *Program Guide* provides information for vendors, laboratories, and other stakeholders regarding the process of evaluation and approval by PCI SSC of payment security devices and reflects a standardized set of:

- PCI PTS Point of interaction (POI) and Hardware Security Module (HSM) Security Requirements,
- Testing methodologies, and
- Approval processes.

Throughout this document:

- "Approved Device List" means the list of PCI SSC-approved PIN Transaction Security Devices appearing on the Website.
- "Participating Payment Brand" means a payment card brand that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC pursuant to its governing documents.
- "PCI SSC" refers to PCI Security Standards Council, LLC, a Delaware limited liability company.
- "Point of interaction (POI) devices" refers broadly to all PIN-acceptance devices used in consumer-facing transactions. Other consumer-facing device types, as delineated in Appendix A, may be included in the POI framework to address any emerging threats to cardholder or other payment card industry (PCI) participants' sensitive data.
- "Hardware security modules (HSMs)" refers to secure cryptographic devices used for PIN processing, card personalization, cryptographic-key management, and data protection.
- "Payment security devices" refers to POI devices and HSMs, collectively.
- "PCI-Recognized Laboratory" (also referred to as a "PTS Lab," "Laboratory" or "Lab") refers to a test laboratory that is at the time currently recognized and approved by PCI SSC for purposes of performing testing of PTS Devices for PTS Program purposes.
- "PIN Transaction Security" refers to the framework within PCI SSC's standards and requirements that deals with the evaluation and approval of payment security devices.
- "Technical FAQ" or "FAQ" means a technical frequently asked question posted and answered by PCI SSC on the Website.
- "Website" refers to the PCI SSC website, currently available at www.pcisecuritystandards.org.

Other terms used herein have the meanings set forth in the Glossary of Terms and Acronyms at the end of the Program Guide.

1.4 About the PCI Security Standards Council

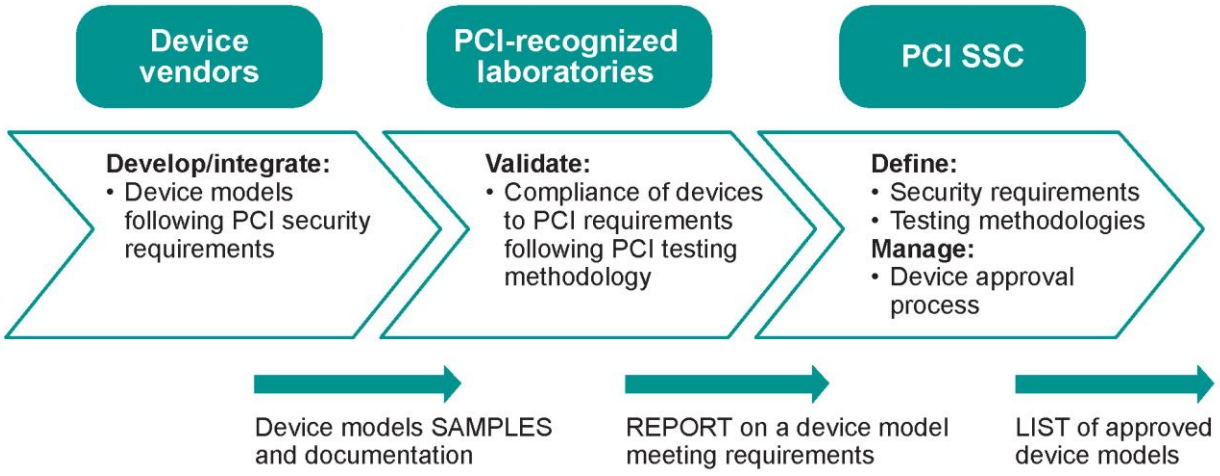
PCI SSC has established the PIN Transaction Security framework to address the security evaluation and approval of payment security devices.

All devices submitted for security evaluation and approval are to be evaluated against the applicable Security Requirements. The Approved Device List provides a full list of payment security devices recognized as meeting applicable PCI PTS Program requirements.

This process helps to ensure that all payment security devices can be evaluated under a common process and is intended to improve overall security for cardholder and other sensitive data. Resulting stakeholder benefits include:

- Customers benefit from a broader selection of PCI SSC-approved payment security devices.
- Merchants, financial institutions, processors, and other third parties gain assurance that they will be using products that have met the applicable Security Requirements.

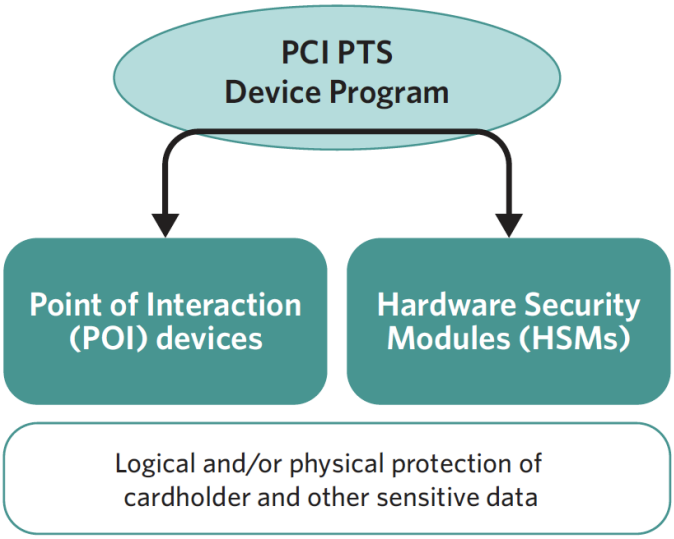
The following picture provides a high-level description of the device security chain.



2 Testing and Approval Process Description

2.1 Overview

The PCI SSC PTS security approval framework addresses the logical and physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs), as indicated in the diagram below.



Except where noted, this document refers to POI devices and HSMs as "payment security devices."

Device vendors wishing to have their device model(s) approved by PCI SSC may contact one of the PCI-Recognized Laboratories and complete the appropriate PCI SSC forms (included in the applicable Security Requirements). The vendor will then submit the device, together with any additional documentation required by the Laboratory, for evaluation and compliance validation against the applicable Security Requirements. Upon completion of the evaluation, PCI SSC will review the evaluation report. When the device model meets applicable PTS Program requirements, it will be approved and listed on the Approved Device List by PCI SSC. An approval letter will be issued confirming successful completion of the process.

2.2 Prior to Testing (POI devices only)

- PCI SSC recommends that the POI device receive EMV Level 1 approval first, if applicable, and then PCI SSC approval prior to submitting it for any appropriate EMV Level 2 testing. (With regards to EMV Level 1 approval, there should be little or no overlap in testing processes with the PCI PTS POI security approval.)
- If the POI device can support both online and offline PIN-entry options, inform the Laboratory to evaluate both at the same time, or have the Laboratory indicate future support for both options in the evaluation report. In order to have the POI device's approval indicate support of both options, the vendor must ensure that after the second PIN-entry option evaluation has been performed, the Laboratory includes both in its report.

2.3 The Modular approach

PCI SSC's modular PTS approach provides a comprehensive evaluation process to address the diversity of payment security device architectures, product options, and integration models. It potentially optimizes evaluation costs and time when laboratories are reviewing non-conventional architectures, the PCI SSC approval of product types, and the maintenance of existing approvals (changes in security components, etc.).

This modular approach supports the submission of devices in accordance with the product types and approval classes defined in Appendix A.

Table 1: Evaluation Modules

In order to capture the diversity of Security Requirements in a single compliance evaluation process by the Laboratory, the PCI PTS POI Security Requirements are split into the following evaluation modules:

Requirements and Evaluation Module Name	Description
Physical Security	Physical security requirements of POI devices.
Logical Security	Logical security requirements of POI devices.
Device Integration Requirements	Requirements for integration of previously approved components aiming to help minimize resulting impairment of overall security as stated in the Security Requirements, including security management requirements applicable to the integrated device.
Communications and Interfaces	The interface of POI terminals to open networks using open protocols.
Life Cycle	Considers how the device is produced, controlled, transported, stored, and used throughout its life cycle.

Each PCI SSC-approved product that incorporates separate modules—such as an EPP, card readers, etc.—must satisfy the corresponding PCI SSC integration requirements.

Products supporting open protocols or seeking to have the secure reading and exchange of data (SRED) designation must be evaluated against the relevant Security Requirements as designated in Appendix B: Applicability of Requirements in the *PTS POI Modular Security Requirements*. See the columns for "Implements Open Protocols" and "Protects Account Data" for requirements that must be met in addition to other applicable requirements.

PCI SSC approval of any device using a communication method that uses a wireless, local, or wide area network to transport data is subject to open protocols evaluation. This includes, but is not limited to, Bluetooth, Wi-Fi, Cellular (GPRS, CDMA), or Ethernet. A serial point-to-point connection would not need to be assessed unless that connection is wireless or through a hub, switch, or other multiport device. In addition, any communication that uses a public domain protocol or security protocol would also be assessed with the applicable Open Protocols requirements.

There are several scenarios where SRED is mandatory for PCI SSC approval. Those scenarios include any device validated to the Non-PED, SCR, or SCRP approval classes, or in some handheld scenarios involving a PIN-entry device attached—e.g., via a sled, sleeve, or audio jack—to a mobile phone, PDA, or POS terminal.

The overall intent of the SRED validation requirement is to help ensure that implementations of account data protection in PCI SSC-approved devices are fully robust as evidenced by validation and approval against the SRED requirements. However, the requirement is not intended to inhibit the vendor from implementing account data protections that, while not sufficient to meet the applicable SRED requirements, may still provide some lesser level of protection for account data. Thus, a vendor may implement account data protections and ***not*** seek SRED as a PCI SSC-approved function.

2.4 Testing Process

Payment security devices are evaluated for PTS Program purposes using the requirements embodied in the *PCI PTS POI Modular Security Requirements* or *PCI PTS HSM Modular Security Requirements*, as applicable. The Laboratory will verify the vendor's "YES" or "N/A" responses in those sections by having the vendor provide additional evidence of conformance to the requirements as stated via information and the required payment security device samples. PCI SSC will not accept any report with "No" as a response.

An "N/A" response is acceptable in two cases:

1. Compliance is achieved by meeting another requirement option, if one exists.
2. The characteristics governed by the requirement are absent in the device. The Laboratory will verify through testing and review that all responses are appropriate.

All N/A responses require reporting on testing performed (including interviews conducted and documentation reviewed) and must explain how it was determined that the requirement does not apply within the scope of the PTS Device evaluation.

Note: *"Not Applicable" cannot be used for implementations that provide only partial aspects of a defined Approval Class to validate the device to that Approval Class. Any product that incorporates separate modules, such as EPPs, card readers, etc., must satisfy the integration requirements. Products are not required to support open protocols or the secure reading and exchange of data; however, if they do, those requirements are mandatory for evaluation and approval.*

Terminal manufacturers may purchase PCI SSC-approved secure components from various vendors and integrate them into their final solutions, which themselves can be approved against the Security Requirements.

The Laboratory will validate payment security devices against the Life Cycle Security Requirements as specified in the *PCI PTS POI Modular Security Requirements* or *PCI PTS HSM Modular Security Requirements.* This is done via documentation reviews and by means of evidence that procedures are properly implemented and used. Any nonconformity with these requirements will be reported to PCI SSC for review. This information is required as part of the approval process.

Table 2: Testing and Approval Process Illustration

The table below and the charts on the following pages outline and illustrate the PCI SSC payment security device testing and approval process.

Process Stage	Resource/Explanation	Illustration
Prior to testing	Testing and Approval Process Description	Figure 1
Obtain appropriate documentation and forms	Detailed Evaluation Process	Figure 2
Contact a PCI-Recognized Laboratory to initiate testing	Preparation for Testing	Figure 2
Sign Vendor Release Agreement (VRA)	Approval Process	Figure 2
Submit documentation and materials	Requirements for Testing	Figure 2
Respond to inquiries from Laboratory	Technical Support throughout Testing	Figure 2
Receive response or approval letter from PCI SSC	Approval Process	Figure 2
PTS Device changes	Changes to a Previously Approved PTS Device	Figure 3

Figure 1: PTS Device Testing Inquiry Flow Chart

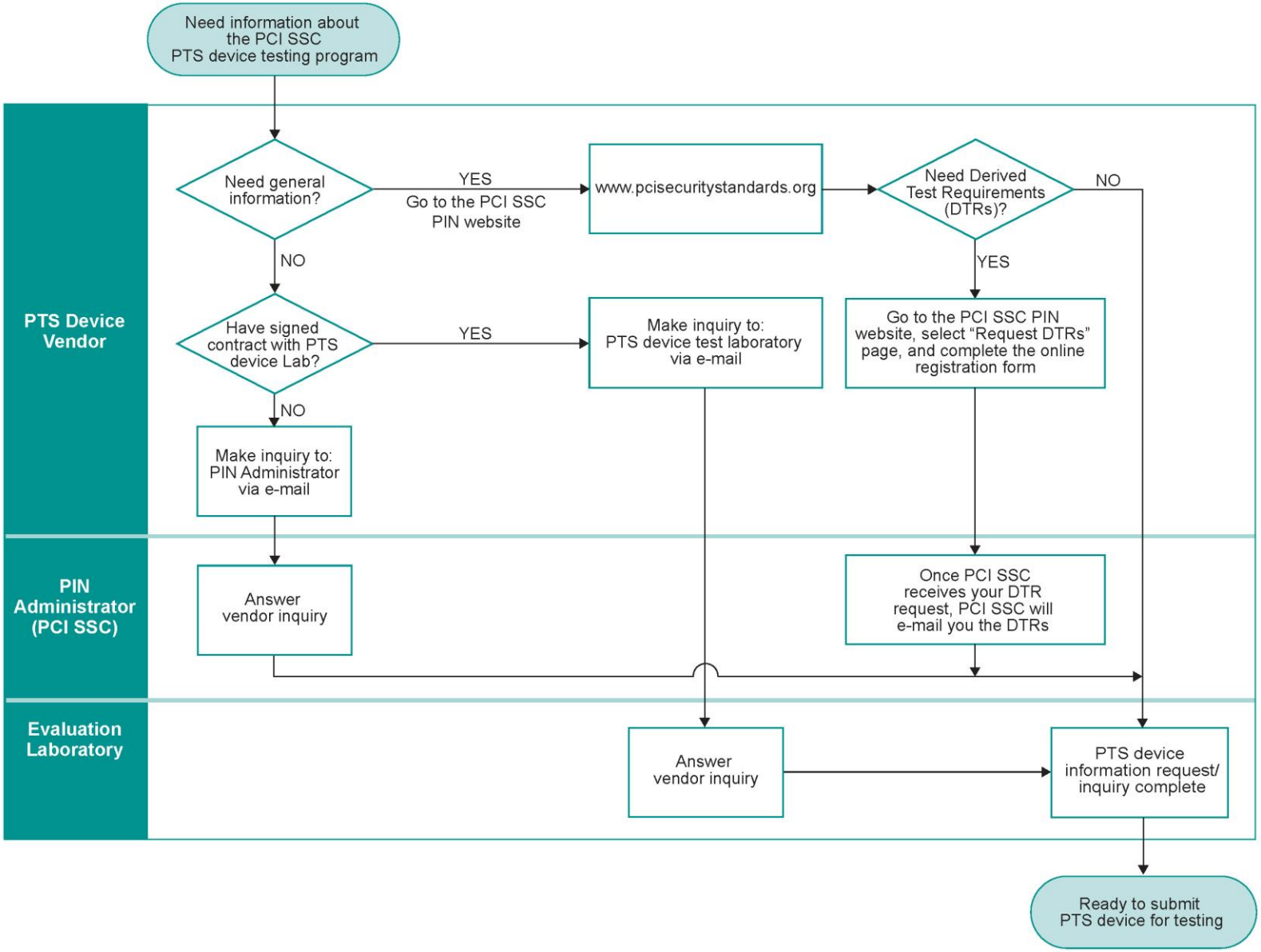


Figure 2: PTS Device Approval Flow Chart

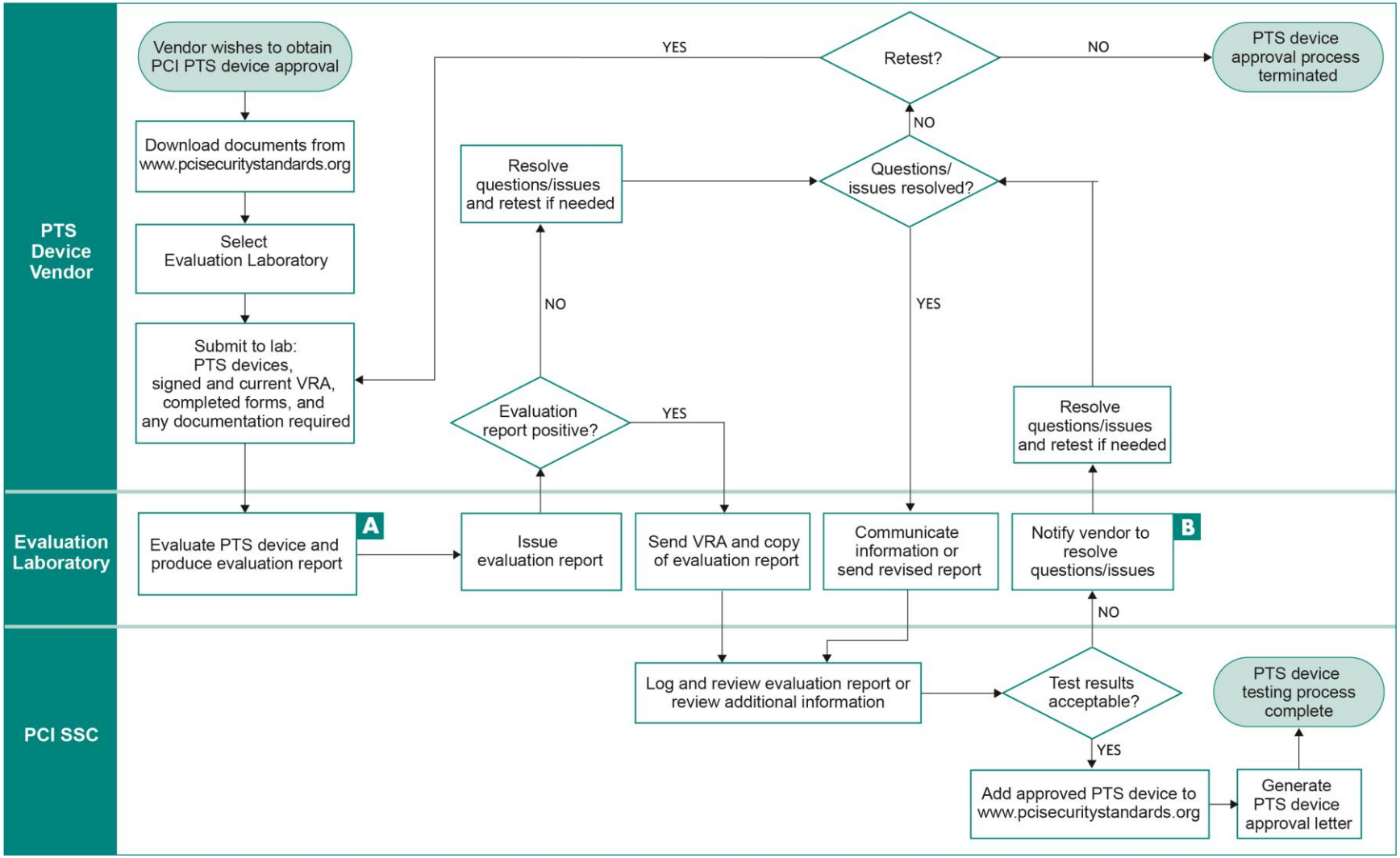
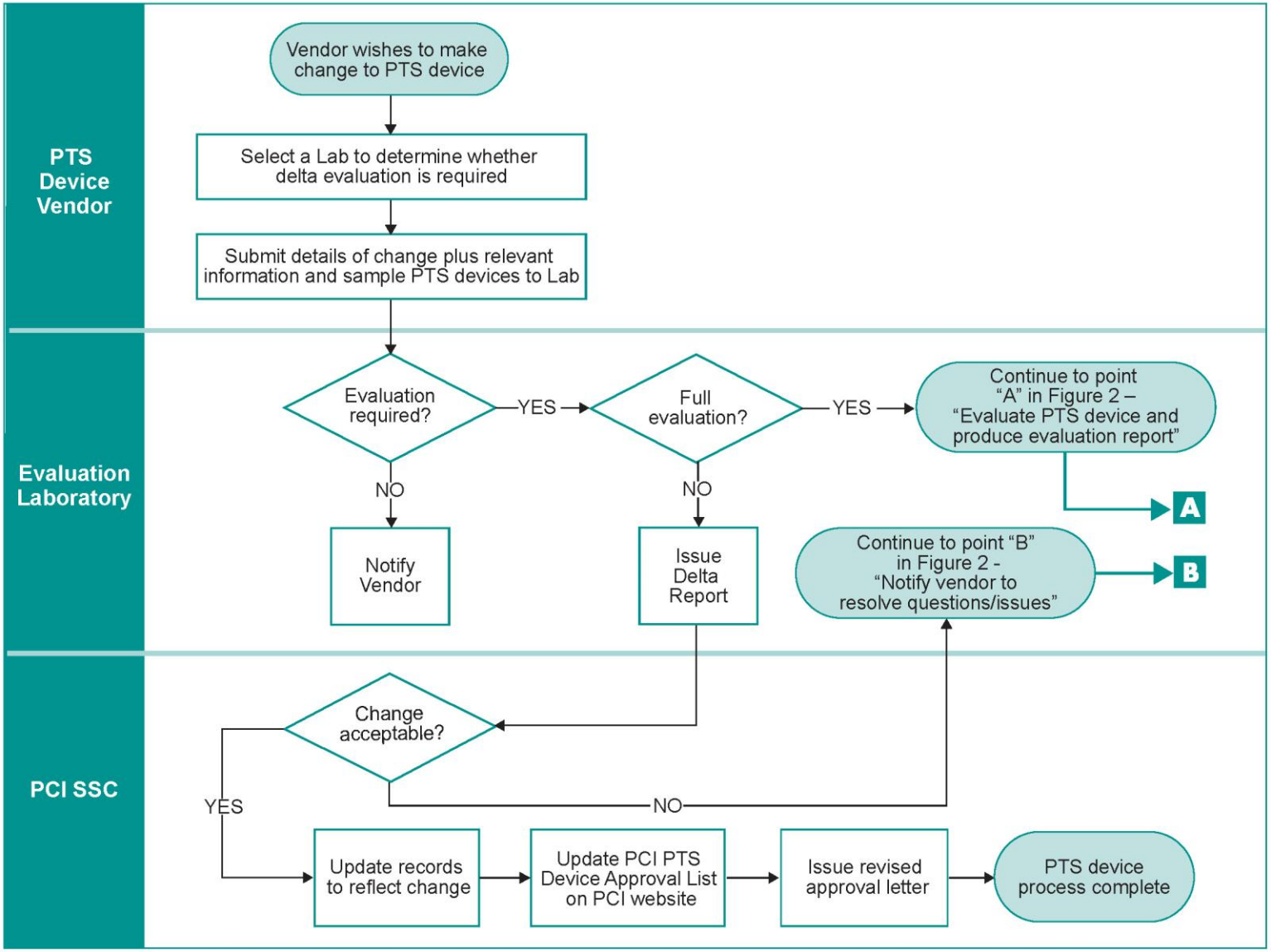


Figure 3: PTS Device Change Request Chart



3 Detailed Evaluation Process

Payment security devices are evaluated against the *PCI PTS POI Modular Security Requirements* or the *PCI PTS HSM Modular Security Requirements*. The Laboratory will evaluate the vendor's responses by having the vendor provide additional evidence of conformance to the requirements—via information and laboratory evaluation of the required payment security device samples. PCI SSC will review the appropriate payment security device evaluation report from the Laboratory. If the results are satisfactory, PCI SSC will approve the payment security device and post the device as a "PCI approved" payment security device on the Website. An approval letter will then be issued to the vendor.

The 'Guidance' in the Derived Test Requirements must be fully considered as required unless they stipulate 'may' or 'should'.

The Technical FAQs are also an integral part of the evaluation process. Technical FAQs are identified by major version of the Security Requirements—e.g., 4.x, 5.x, 6.x. Each Technical FAQ version is specific to the corresponding major version of Security Requirements. For example, Technical FAQs version 6 is specific to Security Requirements version 6.x and only Security Requirements version 6.x, and so on.

The Technical FAQs are periodically updated and are generally effective upon publication. Depending on the nature of the FAQ—e.g., clarification vs. addressing an eminent threat—its applicability may be deferred for a period of time for devices under evaluation at the time of publication.

Modifications, changes, and revisions of PCI SSC-approved devices, termed "deltas," can occur at any time during the product's approval. Devices undergoing delta evaluations must take into account the then current Technical FAQs of the associated major version of Security Requirements only for the Security Requirement(s) that are impacted by the delta change. For example, if a change impacts compliance with requirements B1 and B4, only the then current Technical FAQs associated with B1 and B4 must be considered as part of the delta evaluation.

Devices for which the approval has expired may also undergo delta evaluations. This is because vendors may need to make maintenance fixes to devices that the vendor has already sold but must still provide support for. In addition, vendors may wish to port updated versions of firmware that were approved against newer Security Requirements to products for which the approval has expired. This may occur because customers of a vendor wish to standardize their deployment against a given version of firmware and/or to add functionality to that device.

Upon publication of a major new release—e.g., 4.x, 5.x, 6.x—there will be a 12-month period of overlap with the existing version, beginning the month of the year the newer major version is published. During that period, vendors may choose to submit a device under either version of the applicable Security Requirements. The exception for this is SCRPs, which for new approvals must always use the most current version of the Security Requirements. Twelve months subsequent to publication of the new major release, the older version of Security Requirements will only be available for delta evaluations.

In the year the prior Security Requirements are retired from use, any vendor using those Security Requirements for a new evaluation must have the device in evaluation 60 days prior to the version's retirement date, and PCI SSC must be notified in writing by each PCI-Recognized Laboratory of the specific devices they have under evaluation. The final Laboratory evaluation reports must be received by PCI SSC by the end of that 60-day timeline. If the devices require changes based upon PCI SSC review of the evaluation reports, those changes may be made after that 60-day timeline. However, PCI SSC shall not accept any revised evaluation report subsequent to 60 days past the retirement of the prior major version.

Minor security version updates are generally effective upon publication. Applicability may be deferred for a period of time for devices under evaluation at the time of publication. However, all new and delta evaluations must use the new version within three months of publication of the minor version.

3.1 Required Documentation and Materials

All information and documents relevant to the PTS Program can be downloaded from the Website. All completed forms and questionnaires related to payment security device evaluation must be delivered to a PCI-Recognized Laboratory, not to PCI SSC. Evaluation-specific information should be requested directly from the PCI-Recognized Laboratory.

Examples of documents and items to submit to a PCI-Recognized Laboratory include the following, as applicable for the device approval class:

1. Completed appropriate Security Requirements forms for device.
2. Completed Laboratory vendor questionnaire for device.
3. A user-available security policy for posting with the approval at the Website. The document must contain at a minimum all prescribed information in the applicable Derived Test Requirements.
4. Three (3) working POI devices (for HSMs, consult with the Laboratory) with operator's manual or instructions. Additionally, for POI devices undergoing new evaluations, the vendor shall provide two working devices to the Lab for archiving by PCI SSC as delineated below.
5. The necessary hardware and software accessories to perform simulated PIN-based payment transactions (for HSMs, consult with the Laboratory).
6. Documentation that describes all functions used for data input and output that can be used by third-party application developers. Specifically, functions associated with key management, PIN management, and user interfaces (such as display and keypad) must be described. (An API manual is an example of documentation that could fulfill this requirement.)
7. Documentation that relates to the "process, which can be audited." Examples of such documentation include:
    - Software quality procedures
    - Documentation and software control procedures
    - Change forms
    - Change control logs
    - Change records
8. Instructions and accessories (such as key loaders) that will allow the Laboratory engineers to use all special modes that the payment security device supports—including key loading, key selection, key zeroization, and other key-management and maintenance functions.
9. Additional documentation, such as (a) block diagrams, schematics, and flowcharts, which will aid in the payment security device evaluation, and (b) device form factor and related images for (if approved by PCI SSC) publication on the Approved Device List and related PCI SSC use. The Laboratory may request additional evaluation material when necessary.

Applicable to POI devices only:

Following a successful evaluation, the PTS Lab must provide to PCI SSC two sample devices. The shipping address and local contact are indicated below. Experimental data from certain performed tests must be retained for future provision to PCI SSC on an as-needed basis. This applies to all new evaluations that result in a new approval number. It does not apply to delta evaluations. It also does not apply to a situation where the vendor is merely rebranding another vendor's previously approved product. However, if a vendor is rebranding a product and additionally makes other changes, such as in the firmware, it does apply. They are summarized as follows:

- **Device samples:** Two (2) terminals containing the same keys and applications as those supplied to the PCI-Recognized Laboratory. This includes all approval classes. For large items, please notify via contact details below before shipping. If a device has different variants, the Lab shall send two different variants, selecting those two that most represent the range of all variants. Provision of device samples is a necessary part of a device's approval. These will be securely retained and may be used to assess vulnerability to new attack techniques. If a model is ever compromised in the field, the retained samples may be used to investigate any compromise or security breach.

  Before a letter of approval is issued and listing is posted to the Approved Device List, the Lab must post to the secure PCI SSC web portal made available to the Lab (the "Portal") the shipping company and associated tracking number for the device samples.

- **Robust side-channel testing** is an important part of device evaluation. Relevant side-channel test data (digitally represented waveforms and associated numerical data) produced by an evaluation must be stored by the Laboratory for at least six months following device approval. PCI SSC shall request some or all of this data to be provided as necessary. Labs should communicate with PCI SSC to resolve any questions on this matter.

- **Robust logical-anomalies testing** is an important part of device evaluation. Relevant fuzzing data examples (output data and/or logs, reports, etc.), providing a representative and comprehensible summary of the fuzzing attack test runs must be presented within accompanying evaluation reports, indicating what testing was performed and why, and in sufficient detail to explain testing rationale and conclusions.

Send devices to:	Shipping contact information:
Attn: MasterCard Global Products and Solutions MasterCard Worldwide 5 Booths Park Chelford Road Knutsford Cheshire WA16 8QZ UK	Contact: Mrs. Deborah Corness Telephone: +44 (0)1565 626500 Fax: +44 (0)7738 202 663 E-mail: deborah_corness@mastercard.com

3.2 PTS Attestation of Validation

As of 31 January of each year after which a vendor has received a device approval from PCI SSC, the vendor must complete and submit to PCI SSC an Attestation of Validation (AOV – see Appendix D) for that device, confirming adherence to the Program Guide—i.e., either the hardware and firmware has not been amended or the changes made are either within the wildcard parameters or were submitted for evaluation. The vulnerability process reported on in the AOV must include all physical interfaces and their corresponding logical protocols as defined in D1. For all devices, the vendor must provide evidentiary materials that an auditable record of an ongoing vulnerability assessment process exists by providing a copy of the vendor's sign-off form specified in Requirement E10 of the PTS POI Modular Derived Test Requirements. This applies to all unexpired approvals that exist for the vendor as of 31 December of the prior year. Failure to submit any annual AOV means further report submissions by the vendor will not be processed. An AOV is not required for devices that are End of Life as enumerated in Section 5.

3.3 PTS Device Attestation

Furthermore, vendors may be requested by entities purchasing their devices to complete a PTS Device Attestation—see 3.4 below. This document is for vendors to attest that the hardware and firmware versions of devices that are being purchased are in accordance with the version numbers listed on the Approved Device List for that specific device model name/number.

3.4 Firmware Expiry

Effective with POI v6, firmware expires on 31 December every third year subsequent to the year initially approved. For example, firmware versions approved during 2020 will expire 31 December 2022, 31 December 2025, and 31 December 2028. This expiration is independent of the overall device expiry date—see Section A.12. To remain unexpired, the firmware must be Laboratory evaluated against the following DTRs and the report submitted to and approved by PCI SSC prior to 1 May of the year following expiration. This requires that the reports are submitted to PCI SSC no later than 1 April:

DTR B16	Application Separation
DTR B17	Minimal Configuration
DTR B22	Remote Access
DTR D2	Logical Anomalies
DTR E10	Vendor Vulnerability Assessment Procedures
DTR E11	Vulnerability Assessment of all Interfaces
DTR E12	Vulnerability Disclosure

Note:

This evaluation is in addition to the annual AOV and must consider changes in the vulnerability landscape.

PCI SSC may elect to send an e-mail reminder to the vendor contact (as identified in the most recent approval) within 30 days of the triennial anniversary for a particular firmware version approved under PTS version 6 (or higher).

Firmware expiration evaluations:

- Must use the Firmware Expiration Report template.
- Cannot include other evaluation types e.g., rebranding, hardware or firmware deltas, etc.
- The firmware expiry cannot be past the re-evaluation window, such as shown for firmware version 23.01.xx.xx in the table below.

Where the vendor has multiple firmware versions expiring in different years the evaluations can be combined into one report, effectively synchronizing the expiration dates going forward. But, in order to do so, the following conditions must be met:

- The Firmware Expiration evaluation is specific to an Approval Number.
  - For example, if firmware version v123.45 is used on devices with Approval Number 4-12345 and 4-67890, a separate report is required for each Approval Number.
  - Under a given Approval Number any or all relevant firmware—requiring expiration evaluation—may be included in the evaluation.
- Each firmware version in the report must stand alone—i.e., different sections—in the evaluation report.

Each firmware version on the Approved Device List will have the expiration date appended to the firmware version.

- When a firmware version has gone past the window for re-evaluation and approval, the expiration year will change color to **RED.**
- When a firmware version reaches the end of the expiration year, it will change color to **ORANGE.**

Referring to the table below, which illustrates a device approved in 2020 with a second firmware version added in 2021, assuming the current date is February 2024, the firmware version 23.01.xxx.xx is **RED** because it would have been required to be reviewed and approved by 1 May 2023. The Firmware version 23.02.xxx.xx is **ORANGE** because it is within the re-evaluation and approval window from 31 December 2023 to 1 May 2024.

Company		Firmware Expiry Date	Approval Number	Version	Approval Class	Approval Expiry Date
XYZ Inc.						
Hardware #	A123-xxx-456-xx		4-98765	6.x	PED	30 Apr 2030
	A123-xxx-789-xx					
	A123--0AB-xx					
Firmware #	23.01.xxx xx	(**2022**)				
	23.02.xxx xx	(**2023**)				
Applic #						

4 Preparation for Testing

4.1 Laboratory Services

To facilitate the evaluation process prior to actual testing, a PCI-Recognized Laboratory may offer the following services:

- Guidance on designing payment security devices to conform to the applicable Security Requirements.
- Review of a vendor's payment security device design, response to questions via e-mail or phone, and participation in conference calls to clarify requirements.
- A preliminary physical security evaluation on a vendor's hardware.
- Guidance on bringing a vendor's payment security devices into compliance with the applicable Security Requirements if areas of non-compliance are identified during the evaluation.

Vendors are encouraged to contact a PCI-Recognized Laboratory directly in regard to the above services and any associated fees. However, the Labs **cannot** offer any advice on the actual design of the POI device or HSM.

4.2 PCI-Recognized Laboratories

PCI SSC currently recognizes a series of laboratories for PTS Device testing. The current list of PTS Labs may be found on the Website, on the "Approved PTS Devices" page.

4.3 Test Fees

All device evaluation and testing-related fees and dates are established between the vendor and Laboratory, and the vendor pays all such fees directly to the Laboratory. If a discrepancy requires the vendor to modify the physical design of the payment security device or the firmware, the payment security device must be resubmitted for a new test cycle and the Laboratory will invoice the vendor accordingly.

Note:

The vendor pays all Laboratory testing and evaluation fees directly to the Laboratory.

4.4 Requirements for Testing

As a requirement for testing, the payment security device vendor must provide the appropriate documentation and samples to the Laboratory. See "Required Documentation and Materials" for more information.

The Laboratory may perform a pre-evaluation of a vendor payment security device and decide that there are deficiencies that would prevent an approval. The Lab may then respond to the vendor with a list of all the aspects of the payment security device that should be addressed before the formal testing process begins.

4.5 Test Dates

Vendors submitting devices for testing to a PCI-Recognized Laboratory will be assigned a test date by the Lab. Vendors should notify the Lab directly of any delay in submitting payment security devices for testing.

4.6 Testing Timeframes

A new evaluation can generally start within two weeks of the Laboratory's receiving all items for testing. Timeslots must be scheduled with the Laboratory in advance. The actual evaluation time will vary by the scope of the evaluation and the readiness of the vendor. Evaluations can be performed more quickly if the Laboratory has all of the required documentation and hardware, and if there are not any significant compliance issues.

The testing timeframes are estimates based on the assumption that the payment security device successfully completes testing. If problems are found during testing, discussions between the Laboratory and the vendor may be required. Such discussions may impact testing times and cause delays and/or end the test cycle prior to completion of all tests.

4.7 Test Cycle Definition

All payment security devices are required to complete a test cycle with successful results as part of the PTS Program. A "**test cycle**" is defined as completion of all applicable test procedures performed on a single version of the vendor's payment security device. When a single test cycle is completed without any discrepancies discovered, the vendor is advised that the payment security device has successfully completed a test cycle.

During the testing process, all the applicable test procedures are run according to the applicable PCI SSC *Derived Test Requirements*. Any discrepancies discovered are reported to the vendor. All applicable tests should be run during a single test cycle, unless:

- An application error causes all testing within a portion of the logical software code to function incorrectly, preventing further testing within that area of the application.
- The payment security device contains a catastrophic failure that prevents any continuation of testing.
- Testing exceeds the scheduled test cycle length.
- The vendor requests termination of the test cycle.

If a test cycle has ended with discrepancies discovered, the vendor is notified that the payment security device has failed the test cycle. The Laboratory will issue a final report that addresses the discrepancies.

There is no provision for interrupting the test cycle and re-starting the cycle again at a later date.

4.8 Technical Support throughout Testing

The Laboratory, at its discretion, may seek additional information from the vendor that may resolve the discrepancy. If the discrepancy requires the vendor to modify the physical design of the payment security device or the firmware, the payment security device must be resubmitted for a new test cycle and the Laboratory will invoice the vendor accordingly.

It is recommended that the vendor make available a technical resource person to assist with any questions that may arise during Laboratory testing. During the evaluation, and to expedite the process, the vendor contact should be “on call” to discuss discrepancies and respond to questions from the Laboratory.

Laboratory evaluation work shall occur using approved Laboratory personnel and equipment. Device testing for PTS Program approvals shall be done in the PCI-Recognized Laboratory facility and not at vendor site unless:

- The Laboratory work is in connection with evaluating policies and procedures of the vendor.
- Evaluating Life Cycle Security Requirements.
- Where necessary, to review source code.

Any work completed outside the PCI-Recognized Laboratory facility must be clearly documented in the PTS Device evaluation report.

5 PCI SSC Fees

Vendors are assessed a fee for every new evaluation report received. In addition, vendors will be assessed an annual listing or maintenance fee for each existing PCI SSC approval. These fees are specified on the PCI SSC Programs Fee Schedule on the Website.

5.1 Delinquencies

Vendors who are delinquent in payments to PCI SSC shall not have any reports processed by PCI SSC until they become current. In addition, PCI SSC may assess penalties, fees, and interest for vendors in arrearage.

5.2 New Evaluations

The fee for new evaluations will be a pass-through fee collected by the applicable Laboratory from the vendor. The Laboratory will provide the monies to PCI SSC and recover such fees as part of the Acceptance fee. The fee will be billed quarterly for all new evaluations submitted by the Lab for the preceding three months. Vendors are not billed for PCI SSC review or approval of deltas.

5.3 Initial Evaluations under Major Versions

All initial evaluations under a major version—e.g., 5.x, 6.x, etc.—of the Security Requirements for a given product shall constitute a new evaluation and shall receive a new approval number and be billed accordingly. Delta evaluations are not permitted to take a product previously approved under an earlier major version number—e.g., 5.x—to an approval under another major version number—e.g., 6.x.

5.4 Approval-Listing Fee

The approval-listing fee will be billed semi-annually by PCI SSC. The billing dates shall be set as 1 May and 1 November of every year. Vendors will be billed the full amount for all unexpired PCI SSC approvals existing on 30 April to cover the upcoming period 1 May through 30 April. The 1 November billing will cover any new listings that post from 1 May through 31 October. Vendors with new listings posted during this period will be issued a pro-rated invoice based on the effective date of the listing.

All PCI SSC-approved devices for which the approval has not expired shall be billed an approval-listing fee for all such approvals that existed as denoted above. Vendors shall not be billed the annual listing fee for “End of Life” (EOL) products for which they have notified PCI SSC in writing at least ninety (90) days prior to the billing date of 1 May. An end-of-life product is a product no longer marketed for new deployments as described in Section A.13, “Additional Information.” This applies only to an entire approval, and not individual items within an approval. The notification should be accompanied by a copy of the end-of-life notification sent by the vendor to its customers. The product(s) will continue to be listed by PCI SSC as approved until the natural approval expiration date with notation of the vendor’s cessation of sales for new deployments, unless other reasons—e.g., device compromise—dictate withdrawal of the approval by PCI SSC. In all cases, vendors will not be allowed to manipulate product listings to avoid the listing or maintenance fee.

6 Approval Process

6.1 Vendor Release Agreement and Delivery of Report

Prior to the Laboratory's releasing the evaluation report, the vendor must sign an agreement giving permission for release of the information to PCI SSC for approval consideration. In addition, the vendor must sign the *Payment Card Industry Vendor Release Agreement* ("Vendor Release Agreement" or "VRA"), which is submitted by the Laboratory along with the report. To be accepted by PCI SSC for payment security device approval consideration, the payment security device evaluation reports **must be delivered directly** to PCI SSC by the Laboratories.

Before PCI SSC will review any evaluation report for device approval, PCI SSC must have on file a copy of the then most current version of the VRA on the Website, signed by the applicable vendor. The current version of the VRA is available on the Website. Generally, the vendor will provide its signed VRA to the PTS Lab in connection with the device evaluation process.

Vendors or other third parties licensing PCI SSC-approved products from other vendors to market or distribute under their own names must also sign the most current version of the VRA prior to the issuance of the approval and provide the same to the applicable Laboratory, for the Laboratory to deliver to PCI SSC along with the evaluation report.

Notwithstanding anything to the contrary, if the applicable vendor has the most current version of the VRA from the Website on file and in effect with PCI SSC, that VRA will cover and apply to all vendor products submitted to PCI SSC for approval.

6.2 Roles and Responsibilities

The Laboratory's responsibility and authority are limited to performance of payment security device testing and generation of an evaluation report outlining test results. It is the responsibility and authority of PCI SSC to consider a payment security device for approval based on the results reported by the Laboratory.

It is the responsibility of the Laboratory to ensure evaluation test reports and all other information related to report submissions are accurate, complete, and conform to the PTS Program.

It is the responsibility of the Laboratory and the vendor to allow sufficient time in project scheduling for: device evaluation, report submission for review, inquiry responses and report resubmits, approval process, etc.

6.3 Issuance of Approval

PCI SSC bases its approval solely on the results of the Laboratory evaluation report. All reports, inquiries from report reviewers, and Laboratory responses to inquiries are managed through the Portal. Upon receipt of the test report for a new evaluation, PCI SSC will generally identify any technical issues or questions for resolution by the Laboratory within four weeks (28 calendar days). If the report is deemed by the reviewers as deficient in quality, a reissuance of the report shall be required prior to it being reviewed in its entirety and the report must be redone by the Laboratory and resubmitted, which will restart the entire process. If the reviewers determine a device is inadequate for meeting the applicable security requirements, they will Reject the Device and no further review will occur.

If no issues or questions to the Laboratory are identified within this time frame, PCI SSC shall post the approval information to the Website and issue an approval letter. If questions or issues are identified and sent to the Laboratory, the cycle resets to one week (seven calendar days) after receipt of a complete and acceptable response from the Laboratory. The seven-day reset start does not occur until receipt of an acceptable response for the last open item previously identified. Should additional questions or issues arise, the cycle repeats until a satisfactory response is received, at which time PCI SSC will post the information to the Website and issue the approval letter. In all cases where reports require resubmittal as part of the process of addressing technical issues or questions, the changes to any reports subsequent to the initial report must be done using revision marks—i.e., "redlined."

Additional issues or questions that are raised beyond the initial 28-day period are limited to the same security area(s) for which the technical issues or questions were originally generated. In general, this means limited to the same security requirement(s); however, information provided by the Laboratory may impact other Security Requirements, which would therefore be in scope.

For reports on modifications to existing approved devices, termed "delta" letters or reports, the cycle is an initial 28 calendar days, and PCI SSC shall post the revised information to the Website and issue a revised approval letter unless issues or questions arise in a manner similar to the aforementioned. Delta reports are prepared using the major Security Requirements the payment security device was evaluated against when newly approved. When feasible, changes attributed to the delta should use revision marks on the original report. If not feasible—e.g., because of numerous deltas on the same device—the changes must still be explicitly noted.

The PCI SSC approval letter and device listing on the Website will contain, at a minimum, the following information. Each characteristic is detailed in Appendix A, "Device Listing on PCI SSC Website*."*

- Payment Security Device Identifier
- Approval Number
- Product Type
- Approval Class
- Version
- Expiry Date
- PIN Support (online, offline) – POI only
- Key Management – POI only
- Prompt Control
- Functions Provided
- Approved Components

***Note**:*
PCI SSC will not grant any "partial approvals" based upon the ability of a PTS Device to meet some—but not all—of the applicable required Physical or Logical Security Requirements

For various reasons, including revocation of approval, information on approval letters may become inaccurate. Therefore, the Website is considered the authoritative source and should always be used to validate the approval status of a vendor's product.

6.4 Listing Delay

Vendors may choose to delay listing a newly approved device on the Approved Device List for up to a maximum of six months from date of approval. Written notification on the vendor's letterhead must be submitted to PCI SSC by the vendor through the applicable Laboratory along with the evaluation report. In addition, the Lab must make a notation in the applicable field of the Portal indicating the period of time the device listing should be withheld.

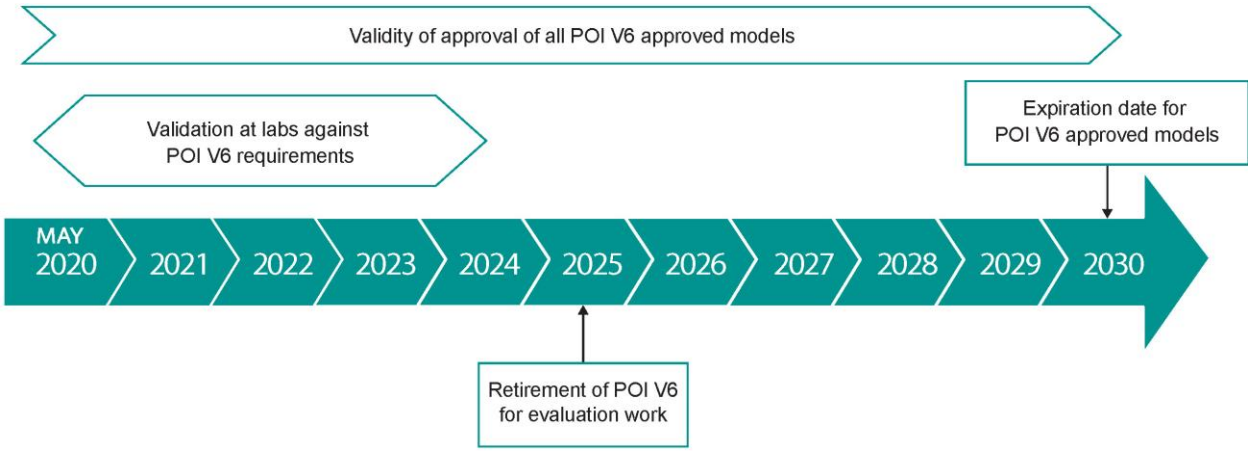
Seven days prior to the listing, a reminder notification will be sent to both the vendor's primary business and technical contacts. The notification will confirm the listing of the device on the Approved Device List and the date to list and instruct the contacts to contact the PTS Program Manager mailbox (PCIPTS@pcisecuritystandards.org) if a change to the listing date is required. Subsequently:

- If there is not a response from the vendor, the device will be listed on the original specified date.
- If the date to list the device falls on a U.S. weekend or holiday, the device will be listed the next following business day.

6.5 Expiry of Approval

In order to maintain the approval of a given approved model, the vendor must have the approved device model re-evaluated against the current version of the applicable Security Requirements before the corresponding device expiration date displayed in the Approved Device List. Upon successful completion, a new approval will be issued under the applicable major version of the Security Requirements.

The following diagram shows the relationship between the expiration of device model tested under Version 6 of PCI PTS POI Security Requirements and its Laboratory testing work.



For devices that embed other PCI SSC-approved devices and are therefore basing their security on these approved components (even partially), the expiration date shall be the earliest among all evaluations, including the embedded device itself.

7 Changes to a Previously Approved PTS Device

If an approved payment security device has undergone changes that may potentially affect security, and/or if the vendor wants the information in its *POI Approval Letter* or *HSM Approval Letter* and on the Website revised, the vendor must submit proper change documentation to the Laboratory for determination whether a full evaluation needs to be performed. The Laboratory will communicate to PCI SSC any information on changes to a previously approved payment security device. PCI SSC will then denote the updates accordingly in its revised *Approval Letter* and on the Website.

7.1 Maintaining Approval

1. **No Impact on Security Requirements: New Testing is Not Required to Maintain Approval**

   If hardware or firmware (including software that impacts security) in the previously approved payment security device is revised, but that revision is deemed to be minor and does not negatively impact security, then documentation of the change can be submitted to the Laboratory for review. It is strongly recommended that the vendor use the same Laboratory that was used for the original evaluation.

   Where appropriate, the Laboratory will issue a letter to PCI SSC describing the nature of the change, stating that it does not impact the POI's or HSM's compliance with the applicable Security Requirements. PCI SSC will then review the letter to determine whether the change has any impact on the approval status of the payment security device.

   If the change is determined not to impact security, the new hardware and/or firmware version number would be considered "Approved" and:

   - The approved payment security device listing on the Approved Device List would be updated accordingly with the new information, and
   - A revised Approval Letter will be issued to the vendor.

2. **Potential Impact on Security Requirements: New Testing is Required to Maintain Approval**

   If changes to the device are determined to impact payment security device security, the device must undergo a security evaluation of those changes. Once that is completed, the Laboratory will submit a new evaluation report to PCI SSC for re-approval consideration. In this scenario, the vendor must first submit documentation of the change to the Laboratory, which will determine (in accordance with applicable Security Requirements) whether the change impacts payment security device security.

7.2 Compound Devices

Compound devices, such as unattended payment terminals, may be evaluated as part of a single evaluation of all applicable components, or may be evaluated with one or more previously approved OEM components. Where a compound device incorporates previously approved components, the following considerations must be made for the evaluation:

- UPT evaluation reports containing separately approved OEM components must at a minimum contain a summary table of all requirements (whether Yes or N/A) of any module that is relevant to the final form factor of the UPT. This table may reference the pertinent OEM component for compliance to any specific requirement.
- All requirements impacted—e.g., additional cardholder input mechanisms, displays, controllers, etc.—by the final form factor of the UPT must be addressed in detail for each impacted requirement.
- Where the Lab evaluating the final form factor is not the same as the Lab that evaluated OEM component(s), the Lab evaluating the final form factor should have access to the OEM component Lab report(s). If those reports are not available—e.g., because submitting vendors are different or for any other reason—the Lab evaluating the final form factor must determine the extent of additional work required.
- If such Lab is unable to rely, where necessary, on information that is available in reports that are not available to the Lab, and the Lab is unable to perform the degree of necessary additional work to achieve such reliance, the Lab evaluating the final form factor must decline the engagement.
- In all cases, PCI SSC may reject the report if, in the judgment of PCI SSC, the report does not contain adequate information to substantiate the conclusions of compliance to overall UPT criteria.

OEM components approved against earlier versions of the applicable Security Requirements are only allowed for use in obtaining an overall UPT approval evaluation without additional testing of those components if they are no more than one major version of the applicable Security Requirements earlier. For example, EPPs evaluated and approved using PCI POI v5.x can be used without additional testing of requirements they have previously met as part of an overall POI v6 evaluation. However, EPPs that were evaluated and approved using PCI EPP v4.x must undergo a full evaluation against all applicable POI v6 requirements.

Additional individual security requirements in POI v6 that were not previously evaluated shall still apply if applicable to the overall UPT evaluation. Furthermore, for devices that embed other PCI SSC-approved devices and are therefore basing their security on these components (even partially), the expiration date shall be the earliest to expire date among all evaluations, including the embedded device itself.

7.3 Rebranding/Licensing

Vendors or other third parties licensing PCI SSC-approved products from other vendors to market or distribute under their own names are not required to pay a new Acceptance fee if the only change is to the name plate. If firmware or other hardware changes are made that require a PCI-Recognized Laboratory to evaluate the changes for potential security impact, the licensee shall be required to pay the new Acceptance fee. In all cases, the licensed device will receive a new approval number, and the licensee vendor or third party shall be billed the annual listing fee for each such approval.

Additional considerations for a third party ("licensee vendor") to license a PCI SSC-approved product (the "original product") from a vendor ("licensor vendor"), whereby the third party wants to distribute it as its own rebranded or licensed product (the "licensee product") include:

1. The licensee vendor cannot directly make the request. The licensor vendor must make the request on behalf of the licensee vendor.

2. All such requests must be received by PCI SSC as a delta request from a PCI-Recognized Laboratory. If the only change is to the nameplate of the product, PCI SSC will not charge a new fee for its review and approval of the licensee product but, as noted above, will charge annual listing fees to applicable vendors for the licensee product and original product.

3. There is no PCI SSC requirement for the licensee product to reference or list the licensor vendor.

4. Products may be licensed from another vendor even if the version of the Security Requirements against which the original product was approved by PCI SSC is retired from use for new evaluations, as long as the approval has not expired.

5. As noted, licensed products requiring physical and/or logical changes will incur a new Acceptance fee. However, as long as the licensor vendor continues the manufacture of the device on behalf of the licensee vendor, the licensee product can be evaluated against the security requirement's version against which the original product was evaluated and approved, even though those requirements may be expired for new approvals.

6. If the licensee vendor wishes to directly manufacture the licensee product or have a third party other than the licensor vendor manufacture the licensee product on its behalf, the product must be reassessed as a new evaluation against the current version of the applicable Security Requirements—unless the licensor vendor can demonstrate that it retains both the intellectual property and engineering control. This is due to the potential for changes in plastics, etc. that may impact the security of the device.

Vendors seeking multiple separate approval listings for their own products are subject to the same conditions for items 2, 3, 4, and 5 as applicable.

Vendors may also make devices that are only intended to be sold and/or manufactured by other vendors. These devices can be evaluated and listed, even though the original vendor may never directly sell these devices, as long as the following criteria are met:

- The device must be fully capable of performing its intended functionality for the approval class it is evaluated against and can be sold as is as a fully functional product. This does not preclude the device requiring additional software such as payment applications, but the firmware of the device must meet all applicable Security Requirements.

- The device must have its own evaluation and product listing on the Approved Device List.

- Each of the second vendors that use the device design and/or manufacture the device must have its own full evaluation (NOT A DELTA) and separate listing for the device on the Approved Device List.

Devices that require additional hardware and/or firmware to operate (such as individual components) are not allowed to be assessed. Those components must be integrated into a device design that meets the required PTS (HSM or POI) Security Requirements.

7.4 Approval Withdrawal

Vendors may submit a request in writing for the withdrawal by PCI SSC of an approval where the vendor has never sold or otherwise deployed any devices of a specific, previously approved model. This applies only to an entire approval, and not individual items within an approval. The request must be made using the PTS Administrative Change Request form via a PCI-Recognized Laboratory. This form is available via the Labs or the PTS Program Manager (pcipts@pcisecuritystandards.org).

7.5 Administrative Changes (Appendix C)

Vendors who have undergone a legal name change or a change of the entity that is the ultimate owner of rights in the applicable listed [devices] for any reason, must update their listing on the Approved Device List by submitting a PTS Administrative Change Request form via a PCI-Recognized Laboratory. Such changes include any change to any part of the vendor's legal name, and any change of the legal entity that is the vendor. For example, changing the vendor's name from ABC Company, Inc. to ABC Company LLC, or from ABC Company, Inc. to XYZ Company, Inc. each would require submission of a PTS Administrative Change Request. Similarly, a PTS Administrative Change Request is required where ultimate ownership rights in applicable listed [devices] has changed.

For vendors who undergo a legal name change, the existing vendor name will be noted as formerly known as (FKA). FKA will also be used where a vendor makes changes to a previously established "DBA" (see Section A.5).

If two existing listed vendors undergo a merger, or if a vendor is involved in a transaction resulting in a change of the legal entity that is the vendor, the name of the vendor may or may not change as a result. In either case, [devices] listed under the vendor before the transaction will be listed under the name of the surviving/new/resulting vendor, with a brief description of the change (e.g., "XYZ Merged with ABC"). In such cases, evidence of the applicable transaction acceptable to PCI SSC is required along with the PTS Administrative Change Request form.

In all cases, the vendor must also submit a new Vendor Release Agreement under the new company name or resulting company, and a revised security policy must be submitted as a delta report via one of the Labs reflecting the applicable change. If the appearance of the device changes to reflect a new name (labels or faceplate), a delta report must be obtained via one of the Labs in accordance with PTS Program delta requirements and procedures.

Vendors who wish to change a model name of an approved device must also use the PTS Administrative Change Request form. However, if any devices have been sold under the prior model name, both names will be listed. Additionally, a new security policy must be created, and either must reference both the new and old names or be listed in parallel to the existing policy. Furthermore, images for the device used on the Website must include both the prior and new models.

The contacts for the PTS Program are as follows: Primary Business, Secondary Business, Technical, and Billing. At minimum, the vendor must provide a primary business and a billing contact. At least two separate points of contact should be provided. Vendors are responsible for keeping their company contact information current to receive important communications from PCI SSC regarding the PTS Program.

Updated contact information should be provided to a PCI-Recognized Laboratory via the PTS Administrative Change Request form.

8 Notification Following a Security Breach or Compromise

Vendors must notify PCI SSC of any security breach or compromise that occurs in relation to an approved payment security device, using the procedures described in this section.

8.1 Notification and Timing

Notwithstanding any other legal obligations the vendor may have, the vendor must immediately notify PCI SSC of any security breach or compromise relating to any vendor-provided:

- Point of interaction or hardware security module
- Key-generation facility
- Key-loading facility

The vendor must also provide immediate feedback about any potential impact this (possible or actual) breach may have had or will have.

Note:

Notification to PCI SSC must take place no later than 24 hours after the vendor first discovers the security breach or compromise.

8.2 Notification Format

The vendor's initial notification of a security breach or compromise must take the form of a phone call to PCI SSC at +1-781-876-8855 (option #3, select prompt for "PIN Program"), followed by an e-mail (pcipts@pcisecuritystandards.org) providing full details of the security breach or compromise.

8.3 Notification Details

Following vendor's initial notification to PCI SSC of a security breach or compromise as described above, the vendor must supply PCI SSC with all relevant information relating to that security breach or compromise. This will include, but is not limited to:

- The number and location of actual products affected
- The number of compromised accounts, (if known)
- Details of any compromised keys
- Any reports detailing the security breach or compromise
- Any reports or evaluations performed to investigate the security breach or compromise

PCI SSC, as agreed within the terms of the *Vendor Release Agreement,* may share this information with PCI-Recognized Laboratories to enable an evaluation of the security breach or compromise to be performed to mitigate or prevent further security breaches or compromises. As a result of this notification, PCI SSC will work with the vendor to correct any security weaknesses and will produce a guideline document to be issued to that vendor's customers, informing them of any potential vulnerability and detailing what actions should be taken in order to mitigate or prevent further security breaches or compromises.

8.4 Actions following a Security Breach or Compromise

In the event of PCI SSC's being made aware of a security weakness or actual compromise related to a specific product, or group of approved products, PCI SSC will take the following actions:

- Notify the Participating Payment Brands that a security weakness or compromise has occurred.
- Attempt to obtain the compromised terminal to evaluate exactly how the compromise occurred. This may include utilizing PCI-Recognized Laboratories.
- Contact the vendor to inform them that their product has a security weakness, or has been compromised and, where possible, share information relating to the actual weakness or compromise.
- Work with the vendor to try to mitigate or prevent further compromises.
- Work with appropriate law enforcement agencies to help mitigate or prevent further compromises.
- Perform evaluations on the compromised product either internally or under the terms of the *Vendor Release Agreement*, using PCI-Recognized Laboratories to identify the cause of the compromise.

8.5 Withdrawal of Approval

PCI SSC reserves the right to withdraw approval of any PTS Device and accordingly update the Approved Device List. Some of the reasons for withdrawal of approval are:

- It is clear that the payment security device does not offer sufficient protection against current threats and does not conform to applicable Security Requirements. If PCI SSC considers that the payment security device has a security weakness or has been compromised, PCI SSC will notify the vendor in writing of its intent to withdraw its approval of that payment security device.
- The vendor either does not meet contractual obligations vis-à-vis PCI SSC or strictly follow the terms of participation in the PTS Program as described in the Program Guide or in the *Vendor Release Agreement.*

9 Legal Terms and Conditions

PCI SSC's approval applies only to payment security devices that are identical to the payment security device tested by a PTS Lab and ultimately approved by PCI SSC. If any aspect of the payment security device is different from that which was tested by the Laboratory and approved by PCI SSC—even if the payment security device conforms to the basic product description contained in the approval letter—then the payment security device model should not be considered approved, nor promoted as approved. For example, if a payment security device contains firmware, software, or physical construction that has the same name or model number as those tested by the Laboratory and approved by PCI SSC, but in fact is not identical to those payment security device samples tested by the Laboratory, then the payment security device should not be considered or promoted as approved.

No vendor or other third party may refer to a payment security device as "PCI Approved," or otherwise state or imply that PCI SSC has, in whole or part, approved any aspect of a vendor or its payment security devices, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in an approval letter signed by PCI SSC. All other references to PCI SSC's approval are strictly and actively prohibited by PCI SSC.

When granted, an approval is provided by PCI SSC to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but the approval does not under any circumstances include any endorsement or warranty regarding the functionality, quality, or performance of any particular product or service. PCI SSC does not warrant any products or services provided by third parties. Approval does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services, which have received an approval, shall be provided by the party providing such products or services, and not by PCI SSC or the Participating Payment Brands.

10 Glossary of Terms and Acronyms

Term	Definition
Approval Class	The approval class describes which evaluation requirements the approved device has been tested against. See Appendix A.
COTS	Commercial-off-the-Shelf device. A mobile device—e.g., smartphone or tablet—that is designed for mass-market distribution and is not designed specifically for payment processing.
CTLS	Contactless
Device	Payment device; may be part of a terminal.
EPP	Encrypting PIN pad; approval class, designating embeddable (OEM) devices to be integrated into a cardholder-operated terminal. See Appendix A.
Evaluation Framework	Set of requirements for vendors, test methodology for laboratories, approval process for products, and PCI SSC approval list pertaining to a given payment security device type (POI device, HSM).
HSM	Hardware security module; approval class aimed at devices supporting a variety of payment processing and cardholder authentication applications and processes. See Appendix A.
Hybrid Reader	A device that incorporates capabilities for the capture of card data from either a magnetic-stripe card or an integrated-circuit card (aka a smart or chip card).
ICCR	Integrated-circuit card reader
KLD	Key-Loading Device
MSR	Magnetic-stripe reader
OEM	Original equipment manufacturer
Payment Security Device	Any complete device (for example, a consumer-facing PIN-acceptance device or an HSM) whose characteristics contribute to the security of retail electronic payments or other financial transactions.
PED	PIN entry device; approval class for devices with PIN-entry and PIN-processing ability, either attended or unattended, whose primary purpose is to capture and convey the PIN to an ICCR and/or to another processing device, such as a host system. A PED must have an integrated display unless dedicated to PIN entry only. See Appendix A.
POI	Point of interaction
POI Device	Device used in the point of interaction with a consumer.
Product Type	The product type describes whether or not the device is a module to be integrated (OEM).

Term	Definition
PTS	Acronym for PIN Transaction Security, the PCI SSC evaluation, security, testing, and approval framework for payment security devices, including POI devices and HSMs.
PTS Device	A POI device or HSM as defined in A.10.
PTS-HSM	The sub-framework of the PCI SSC PTS Device security framework that addresses the security of HSMs.
PTS-POI	The sub-framework of the PCI SSC PTS Device security framework that addresses the security of consumer-facing devices.
PTS Program	The program operated by PCI SSC for purposes of supporting the PTS evaluation, security, testing, and approval framework.
RAP	Remote Administration Platform for HSMs
Remote Administration Solution	A non-console-based mechanism for the administration of HSMs that may involve the use of RAP devices or smart card-based implementations.
SCR	Secure Card Reader approval class
SCRP	Secure Card Reader PIN approval class
SPoC	Software-based PIN-entry on COTS
SRED	Secure Reading and Exchange of Data
Terminal	Commercial device with a business function. It may be dedicated to payment (POS terminal with integrated or separate PIN pad) or to product-dispensing (for example, an ATM or petrol-dispensing self-service).
Test Cycle	Completion of all applicable test procedures performed on a single version of the vendor's payment security device.
UPT	Unattended payment terminal; approval class, designating cardholder-operated payment devices (self-service) that read, capture, and transmit card information in conjunction with an unattended self-service device. See Appendix A.

Appendix A: Device Listing on PCI SSC Website

Listed below are the characteristics of a device listing on the Approved Device List.

A.1 Point of Interaction (POI)

For purposes of these requirements, a **POI device** is defined as:

> *A device that provides for the entry of PINs and/or account data, used for the purchase of goods or services or dispensing of cash. An approved POI has met all of the applicable PCI PTS POI requirements for PIN entry and/or account-data entry and has a clearly defined physical and logical boundary for all functions related to PIN entry.*

A PIN entry device (PED) is a class of POI that supports the secure acceptance of a cardholder's PIN.

In addition, non-PIN-acceptance POI devices can be validated and approved if compliant to the Secure Reading and Exchange of Data (SRED) requirements, and if applicable, to the Open Protocols requirements. These devices shall be explicitly noted as not approved for PIN acceptance.

Secure Card Readers and Secure Card Readers – PIN must be validated to the requirements as delineated in *Appendix B: Applicability of Requirements* of the *PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements.*

All approval classes are subject to the Life Cycle Security Requirements.

A POI device may be standalone and not embeddable, in which case the PED approval class may be applicable. This class may apply to both attended and unattended. However, vendors may decide to list an unattended terminal under the UPT class, when meeting the appropriate requirements.

If the POI device is designed to be embedded into a wider set—e.g., vending machine or ATM—then EPP or PED approval class would apply. In such case, there can be other functionalities present besides PIN capture and conveyance—e.g., display, card reader. Devices entering this category will have the product type noted with the word "OEM" on the listing, to unambiguously advertise the modular nature.

POI devices that combine goods—e.g., petrol—or services (ticketing machine) delivery with PIN-based payment are eligible for the UPT approval class. These POIs can possibly include approved OEM modules.

POI devices submitted for testing must be properly identified so that PCI SSC participants' customers or their agents can be certain of acquiring a POI that has been approved by PCI SSC.

A.2 Hardware Security Module (HSM)

For purposes of these requirements, an **HSM** is defined as:

> *A physically and logically protected hardware device that provides a secure set of cryptographic services. It includes the set of hardware, firmware, software, or some combination thereof that implements cryptographic logic, cryptographic processes, or both, including cryptographic algorithms.*

Furthermore, this document introduces a two-tier approval structure for HSMs. These tiers differentiate only in the Physical Security Requirements section as delineated in the *PCI PTS HSM Modular Derived Test Requirements.* HSMs may be approved as designed for use in controlled environments as defined in *ISO 13491-2: Banking — Secure Cryptographic Devices (retail)* or approved for use in any operational environment. These categories are:

- **Restricted –** Approval is valid only when deployed in Controlled Environments or more robust —e.g., Secure Environments—as defined in ISO 13491-2 and in the device's PCI HSM Security Policy.
- **Unrestricted –** Approval is valid in any environment.

A.3 Devices with Expired Approval

These are devices whose approval has expired as delineated in the "Expiry Date" section of this document. For specific information regarding Participating Payment Brand usage mandates for expired devices, please contact the Participating Payment Brand(s) of interest.

A.4 Device Identifier

The Device Identifier is used by PCI SSC to denote all relevant information that is representative of an approved point of interaction or hardware security module, and consists of:

- Vendor Name
- Model Name/Number
- Hardware #
- Firmware #
- Application #, if applicable

The model name/number and vendor name must be visually and distinctly present on the device and not be part of a larger character string. The device must show the version numbers of hardware and firmware in accordance with the device's approval, reflecting information on the Approved Device List. The model name and hardware version must be retrievable from the device by a query. The hardware number must be shown on a label attached to the device and be distinctly identified as the hardware version—e.g., HW#, HWID, etc. The firmware and application version numbers, and optionally the hardware version number, must be shown on the display or printed during startup or on request. This includes all Security Requirements addressed in testing, including SRED and Open Protocols. If the hardware version label is not visible when the device is installed, such as on an EPP in an ATM, other means must exist to display the version number. This shall be illustrated by photographic evidence provided in the evaluation report.

In order to ensure that the payment security device has received an approval, acquiring customers or their designated agents are strongly advised to purchase and deploy only those payment security device models with the information that matches exactly the designations given in the components of the Point of Interaction Device Identifier or the Hardware Security Module Identifier.

Table 3: Example of a Device Identifier (five components)

Component	Description
Vendor Name	Acme
POI Model Name/Number	PIN Pad 600
Hardware #	NN-421-000-AB
Firmware #	Version 1.01
Application #	PCI 4.53

The Device identifier will be included in the approval letter and on the Website. If an identical payment security device is used across a family of devices, vendors are cautioned against using a Hardware # (see below) that may restrict approval to only that payment security device model.

A.5 Vendor Name

Vendors shall be listed by their full legal name. A vendor's listing may also include its trade name, alternate name, or doing-business-as name (each a "DBA"). If the vendor requests the listing of a DBA, the vendor must provide a government approved DBA or similar authorization acceptable to PCI SSC. The vendor shall be listed by the full legal name, followed by the DBA.

A.6 Model Name/Number

The model name/number cannot contain any variable characters. All devices within a device family that are intended to be marketed under the same approval number must be explicitly named, and pictures of those devices presented in both the evaluation report and for display on the Approved Device List. The vendor cannot use an identical model name for more than one device approved by PCI SSC under a given major version release of the applicable Security Requirements. The vendor cannot choose to use the name of an approval class for which the device is not approved as part of the device's model name.

A.7 Hardware

Hardware # represents the specific hardware component set used in the PCI SSC-approved payment security device. The fields that make up the Hardware # may consist of a combination of fixed and variable alphanumeric characters. Variable characters are not permitted for any physical or logical device characteristics that impact security. Device characteristics that impact security must be denoted using fixed characters. The use of variable characters shall be validated by the Laboratory so as to not impact security.

Note:

The firmware version number may also be subject to the use of variables in a manner consistent with hardware version numbers.

A lower-case "x" is used by PCI SSC to designate all variable fields. The “x” represents fields in the Hardware # 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, etc.

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

Note:

Vendors may have produced payment security devices with the same model name/number (prior to validation of compliance by the Laboratory) that do not meet the applicable payment security device Security Requirements.

Options that cannot be a variable character include those that directly pertain to meeting applicable Security Requirements. For example, requirements exist for magnetic-stripe readers (MSRs) and integrated circuit card readers (ICCRs). A variable character cannot be used to designate whether a device contains a MSR or an ICCR. A requirement exists for the deterrence of visual observation of PIN values as they are being entered by the cardholder, which can be met by privacy shields or the device’s installed environment or a combination thereof. It is not appropriate to wildcard variable options if the device supports more than one means of observation deterrence.

If a device supports SRED or OP, some options that might normally be acceptable for identification by a wildcard variable would not be permitted. Examples include the addition of contactless readers or the inclusion of different communication packages. In such cases, the specific configurations validated by the PCI-Recognized Laboratory must be explicitly noted on the approval.

For HSMs, an example would be non-PCI mode—e.g., FIPS—or PCI mode support. If wildcards are used, the specific configurations validated by the PCI-Recognized Laboratory must be explicitly noted on the approval.

In addition, all options, both security and non-security relevant, must be clearly defined and documented as to the options available and their function in the evaluation report. Security-relevant options must be exhaustively defined and documented in the security policy. For non-security options, the security policy must include a description of the option, but not a full list of all possible values.

Table 4: Examples on the Use of Hardware #s

Hardware # of Payment Security Device in Approved Device List	Comments
NN-421-000-AB	Hardware # NN-421-000-AB of the Device Identifier does not employ the use of the variable "**x**." Hence, the payment security device being deployed must match the Hardware # exactly for the PTS Device to be considered an approved payment security device (hardware component).
NN-4**x**1-0**x**0-A**x**	Hardware # NN-4**x**1-0**x**0-A**x** of the Device Identifier uses the variable "**x**." Hence, the payment security device being deployed must match the Hardware # exactly in only those position(s) where there is no "**x**."
Actual Hardware # of POI Supplied by Vendor	**Comments**
NN-421-090-AC	If the PCI SSC Website lists NN-421-000-AB as the Hardware # in the Device Identifier, then the payment security device with the Hardware # NN-421-090-AC **cannot** be considered an approved payment security device (hardware component). However, if the PCI SSC Website lists NN-4**x**1-0**x**0-A**x** as the Hardware # in the Device Identifier, then the payment security device with Hardware # NN-421-090-AC **can** be considered an approved payment security device (hardware component).
NN-421-090-YC	If the PCI SSC Website lists NN-4**x**1-0**x**0-A**x** as the Hardware # in the Device Identifier, then the payment security device with the Hardware # NN-421-090-YC **cannot** be considered an approved payment security device (hardware component).

A.8 Security Policy

The device vendor provides a user-available security policy that addresses the proper use of the device in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy must define the roles supported by the device and indicate the services available for each role in a deterministic tabular format. The device is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the device are those allowed by the policy.

A.9 Approval Number

Approval numbers are assigned by PCI SSC at the time of approval and remain the same for the life of the device's approval.

A.10 Product Type

The product type gives an insight on both the approval class of a device, and whether the device is a module to be integrated (OEM) or is ready-to-deploy equipment. The product type shall be prefixed with **"OEM"** if the approved device is clearly designed to be integrated into a wider set, or as a non-PED to clearly differentiate a non-PIN-acceptance POI device from a PIN-acceptance POI device.

Vendors manufacturing self-contained OEM products that are "bolt on" or drop in type modules—i.e., fully functional PED modules integrating all required components—for UPTs may choose to partner with final form factor vendors of those UPTs—e.g., automated fuel dispenser or kiosk vendors. The OEM vendor's product may meet most of the overall UPT Security Requirements, and the OEM vendor may submit that product in conjunction with additional information from the final form factor vendor on behalf of that vendor, such as AFD or kiosk case design, to the Laboratory for evaluation as an UPT.

The OEM vendor's product cannot receive a UPT approval because the actual final form factor product may have additional cardholder interfaces—e.g., displays or data input devices—or other characteristics that are within the scope of the UPT Security Requirements. The final form factor vendor's product would receive the UPT approval. The OEM vendor's product would be assigned a separate approval number and would be listed separately; in addition, it would be listed as an approved component of the UPT product, similar to the way other OEM products are listed.

A.11 Approval Class

The **Approval Class** is used by PCI SSC to ensure that its payment security device approvals accurately describe today's ever-evolving designs, architectures, and implementations. All POIs and HSMs approved by PCI SSC in the framework of the PTS Program, regardless of the designated Approval Class, carry PCI SSC's full approval status. Financial institutions, or their designated agents—e.g., merchants or processors—should make sure that they understand the different classes, as they represent how the payment security device has met the applicable Security Requirements.

Table 5: Approval Class Descriptions

Approval Class	Description	Potential Features *(see Table 7 in A.14 below for detail)*
EPP	An approval class aimed at secure PIN entry and encryption modules in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an unattended PIN-acceptance device for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary and a tamper-resistant/responsive or tamper-evident shell. At a minimum, a device submitted for EPP approval must contain a PIN-entry keypad along with its built-in secure cryptographic module. Original equipment manufacturers (OEMs) or providers of encrypting PIN pads (EPPs) to unattended PIN-acceptance device manufacturers—e.g., ATMs or UPTs—and other self-service device types can submit an EPP for Laboratory testing and approval. As an integral component of a complete and fully functional POI, an approved OEM EPP can be used in another payment device such as an ATM or UPT to minimize testing redundancy. However, UPTs using an approved EPP will still be required to go through a Laboratory evaluation to obtain overall approval of the UPT.	PIN support PIN Encryption Key Management SRED Key Management Prompt Control PIN-Entry technology ICCR MSR CTLS Display SRED OP Supports ISO Format 4 Interface Isolation – Bluetooth Interface Isolation – Wi-Fi
HSM	HSMs may support a variety of payment processing and cardholder authentication applications and processes. The processes relevant to the full set of requirements outlined in this document are: ▪ PIN Processing ▪ 3-D Secure ▪ Card Verification ▪ Card Production and Personalization ▪ EFTPOS ▪ ATM Interchange ▪ Cash Card Reloading ▪ Data Integrity ▪ Chip Card Transaction Processing	Remote Administration Restricted Unrestricted Supports ISO Format 4 Remote-managed HSM

Approval Class	Description	Potential Features *(see Table 7 in A.14 below for detail)*
KLD	An SCD that may be used for securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. Key-transfer and loading functions include the following: ▪ Export of a key from one secure cryptographic device (SCD) to another SCD in clear-text, component, or enciphered form; ▪ Export of a key component from an SCD into a tamper-evident package—e.g., blind mailer; ▪ Import of key components into an SCD from a tamper-evident package; ▪ Temporary storage of the key in clear-text, component, or enciphered form within an SCD during transfer.	N/A
Multi-tenant HSM	HSMs intended for multi-tenant usage—i.e., multi-organizational usage.	Remote Administration Restricted Unrestricted Supports ISO Format 4 Remote-managed HSM
Non-PED	An approval class of POI devices that does NOT allow the entry of a PIN for a payment card transaction. This class is for ALL POI devices or device combinations, attended or unattended, which do not support PIN-based payment transactions. OEM product types may require further integration into a POI terminal. The device or any combination of hardware can be used as evaluated to operate in an acquirer network. The firmware must include an acquirer-approved payment application necessary for its operation. Non-PED POI devices intended for use in an attended environment must be self-contained, fully functional units that are capable of processing payment transactions and must include a merchant interface necessary for their operation. Non-PED POI devices (terminals) are validated to the Secure Reading and Exchange of Data requirements and, if applicable, the Open Protocols requirements. These non-PED POI devices are NOT approved for PIN acceptance.	SRED Key Management ICCR MSR CTLS SRED OP Interface Isolation – Bluetooth Interface Isolation – Wi-Fi

Approval Class	Description	Potential Features *(see Table 7 in A.14 below for detail)*
PED	An approval class for POI devices, originally designed for supporting payment with PIN entry, and dedicated to payment. A PED must have an integrated display unless dedicated to PIN entry only. This class may cover both attended and unattended environments and OEM or stand-alone products.	PIN support PIN Encryption Key Management SRED Key Management Prompt control PIN-Entry Technology ICCR MSR CTLS Display SRED OP Supports ISO Format 4 Interface Isolation – Bluetooth Interface Isolation – Wi-Fi
RAP	This is for platforms that are used for remote administration of HSMs. Such administration includes device configuration and may also include clear-text cryptographic key-loading services as part of the same SCD.	N/A

Approval Class	Description	Potential Features *(see Table 7 in A.14 below for detail)*
SCR	An encrypting card reader that either: ▪ Is intended for use with a non-secure device, such as a mobile phone or other device; or ▪ May be defined as an OEM product type to be integrated into a POI terminal or ATM. OEM product types may contain a payment application and be capable of stand-alone usage or can be a slave device to process account data securely (SRED) and, if applicable, perform offline PIN verification and require connection to a secure module, terminal, or PIN pad. A Secure Card Reader can be: ▪ A hybrid card reader ▪ A magnetic-stripe-only reader ▪ A contact chip-card-only reader ▪ A contactless-only reader SCRs must meet as applicable the ICCR, CTLS, and/or MSR requirements designated in Appendix B of the *PCI PTS POI Security Requirements* and the Secure Reading and Exchange of Data requirements. If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), then requirements specified in Open Protocols requirements must also be met. Other requirements, such as B1, Self-tests, and B9, Random Numbers, may apply depending on device functionality. If a SCR supports offline PIN authentication via an ICCR component or it formats and encrypts a PIN block to send online directly to the host—it must be validated in conjunction with a specific PIN entry device—e.g., PED or EPP—to validate the security of the interaction, including the establishment of the keying relationship. The PIN entry device must either be previously approved or obtain approval concurrent with the SCR in the same or a concurrent, separate Laboratory evaluation. PIN Encryption Key Management is only applicable where the SCR does PIN translation in connection with sending the PIN online to a host and must meet the determining keys requirements.	PIN Support PIN Encryption Key Management SRED Key Management ICCR MSR CTLS SRED OP Supports ISO Format 4 Interface Isolation – Bluetooth Interface Isolation – Wi-Fi

Approval Class	Description	Potential Features *(see Table 7 in A.14 below for detail)*
SCRP	An encrypting card reader that is intended for use with a commercial-off-the-shelf (COTS) device, such as a mobile phone or tablet. A Secure Card Reader PIN (SCRP or SCR-PIN) can be: ▪ A contact chip-card-only reader ▪ A contactless-only chip-card reader ▪ A reader supporting both contact and contactless chip card functionality ▪ A hybrid reader that includes a magnetic stripe card reader and contact and/or contactless chip card functionality SCRPs must meet as applicable the ICCR requirements designated in Appendix B of the *PCI PTS POI Security Requirements* and the Secure Reading and Exchange of Data requirements. If the device is capable of communicating over an IP network or uses a public domain protocol (such as but not limited to Wi-Fi or Bluetooth), it must meet the applicable Open Protocols requirements. Other requirements in the Physical and Logical sections may apply depending on device functionality. SCRPs perform PIN translation from PIN blocks received from the payment application on the COTS device to a PIN block either for conveyance to the processing host or for offline verification to the contact chip card.	PIN support PIN Encryption Key Management SRED Key Management ICCR MSR CTLS SRED OP Supports ISO Format 4 Interface Isolation – Bluetooth Interface Isolation – Wi-Fi
UPT	The UPT class of device covers cardholder-operated payment devices that read, capture, and transmit card information in conjunction with an unattended self-service device, including, but not limited to, the following: 1. Automated Fuel Dispenser 2. Ticketing Machine 3. Vending Machine UPTs may have a compound architecture directly combining payment and the delivery of services and/or goods.	PIN support PIN Encryption Key Management SRED Key Management Prompt control PIN-Entry Technology ICCR MSR CTLS Display SRED OP Supports ISO Format 4 Interface Isolation – Bluetooth Interface Isolation – Wi-Fi

A.12 Version

Version refers to the version of the Security Requirements the device has been evaluated against. Each approval class may follow its own version release schedule.

A.13 Expiry Date

The expiration date for PCI SSC-approved devices is the date upon which the device's approval expires. All device approvals expire in accordance with the schedule below.

Table 6: Approval Expiry Dates

Requirements Version Used During Evaluation at Laboratory	Expiration of Requirements	Approval Expiration of Device Models
Version 4.x of *PCI PTS HSM Modular Security Requirements*	December 2025	April 2032
Version 6.x of *PCI PTS POI Modular Security Requirements*	June 2025	April 2031
Version 5.x of *PCI PTS POI Modular Security Requirements*	June 2021	April 2026
Version 3.x of *PCI PTS HSM Modular Security Requirements*	December 2022	April 2026
Version 4.x of *PCI PTS POI Modular Security Requirements*	September 2017	April 2024
Version 2.x of *PCI PTS HSM Security Requirements*	June 2017	April 2022
Version 3.x of *PCI PTS POI Modular Security Requirements*	April 2014	April 2021
Version 1.x of *PCI PTS HSM Security Requirements*	April 2013	April 2019
Version 2.x of *PCI PED Security Requirements* or *PCI EPP Security Requirements*	April 2011	April 2017
Version 1.x of *PCI UPT Security Requirements*	April 2011	April 2017
Version 1.x of *PCI PED Security Requirements* or *PCI EPP Security Requirements*	April 2008	April 2014

PCI SSC device approvals expire six years past the effective date of a subsequent major (5.0, 6.0, etc.) update of the applicable Security Requirements.

POI v6 firmware expires three years from the date of approval but shall not expire past the overall approval expiration of the device.

A.14 Specific Features per Approval Class

Table 7: Specific Features

Feature and Applicability	Description
PIN Support (EPP, PED, SCR, SCRP, UPT)	**"PIN support"** denotes the type of PIN entry verification that can be supported by the POI. "**Online**" represents that the POI has the capability to support online PIN verification by the payment card's issuer or its designated processor. To pass testing, POIs that support online PIN entry must support the use of TDES or AES to protect the PIN. Additionally, if the PIN needs to be protected during transport in nonintegrated offline POIs, then the POI must support the use of TDES or AES for that channel. "**Offline**" means that the POI has the capability to support offline PIN verification by the payment card's integrated chip. Unless otherwise noted, the "Offline" designation, without any suffix, in the *Approved Device List* represents that the POI has the capability to support both plaintext and enciphered offline PIN verification. The "Offline (p)" designation with the "(p)" as a suffix represents that the offline POI has the capability of performing only plaintext offline PIN verification. ***Note:*** *All newly approved offline PIN verification POIs must support both plaintext and enciphered PIN verification.* However, under current testing, all newly evaluated offline POI devices must support both plaintext and enciphered PIN verification. SCRs or other POI devices that include an ICCR or hybrid reader must have an "Offline" designation in order to be used for offline PIN acceptance.

Feature and Applicability	Description
PIN Encryption Key Management (EPP, PED, SCRP, SCR, UPT)	**"PIN encryption key management"** denotes whether the Laboratory has successfully evaluated the payment security device to support the use of Triple DES (**TDES**) or **AES** for PIN encryption for online PIN. TDES requires use of at least a double-length key. A **MK/SK** (master key, session key), **DUKPT**, and/or **Fixed** designation denote that the device has been evaluated successfully to support the implementation of TDES for that particular key-management method(s). Where AES is used, that will be explicitly noted in conjunction with the **MK/SK**, **DUKPT** and/or **Fixed** Key methodologies. ***Note:*** *DUKPT is the only unique key per transaction (UKPT) algorithm (ANSI X9.24) that PCI SSC recognizes and approves; all other forms of UKPT tested by the Laboratory will not be depicted in the approval letter or on "Approved PTS Devices" on the Website.* ***Note:*** *Fixed Key is not allowed for POI v6 and higher devices.* This is for POI devices supporting the entry of online PINs, and in general, this will be N/A for devices in the Non-PED or SCR approval classes and will be N/A for offline PIN-only devices. SCRPs can indirectly support online PIN in connection with mobile-based solutions via PIN translation. PIN Encryption Key Management is only applicable for SCRs where the SCR does PIN translation in connection with sending the PIN online to a host. ***Note:*** *POI v5 and v6 devices used for online PIN must support ISO PIN Block Format 4 (AES).*
SRED Key Management (EPP, PED, SCR, SCRP, UPT)	**"SRED key management"** denotes whether the Laboratory has successfully evaluated the payment security device to support the use of Triple DES **(TDES**) or **AES** for Account Data encryption. TDES requires use of at least a triple-length key or DUKPT for account data encryption. A **MK/SK** (master key, session key), **DUKPT** and/or **Fixed** designation denote that the device has been evaluated successfully to support the implementation of TDES for that particular key-management method(s). Where AES is used, that will be explicitly noted in conjunction with the **MK/SK**, **DUKPT** and/or **Fixed** Key methodologies. ***Note: Fixed*** *Key is not allowed for POI v6 and higher devices.* Format-preserving encryption (**FPE**) shall be denoted where one of the ANSI, ISO or NIST approved algorithms are used. ***Note:*** *The FPE notation is only presented for POI v6 and higher devices.*

Feature and Applicability	Description
Prompt Control (EPP, PED, UPT)	▪ **Vendor-controlled:** The end-user, acquirer, or reseller cannot modify the POI's firmware or POI's payment application to make changes to the device's prompts or PIN-entry controls. Only the POI's original equipment manufacturer has the capability to modify the prompts and controls for PIN entry. ▪ **Acquirer-controlled:** The original equipment manufacturer has shipped the POI with mechanisms for controlling the POI display and its use in place. These mechanisms can be employed to unlock the POI for updates of the prompts by the acquirer, using proper cryptographically controlled processes as defined in the applicable POI security requirement. The reseller or end-user, if authorized by the acquirer, can also make updates using proper cryptographically controlled processes. Not applicable for devices without a display. Devices must be deployed locked. In any case, the acquiring customer is **always** responsible to ensure that appropriate processes and documented procedures are in place to control the POI display and usage.
PIN-Entry Technology (EPP, PED, UPT)	**"PIN-entry technology"** denotes which technology is implemented in order to capture the cardholder PIN. The value for this field can be: ▪ **Physical keypad:** Set of buttons arranged in a block which bears digits and optionally letters, in conformance with ISO 9564. ▪ **Touch screen:** Display that can detect the presence and location of a touch within the display area and enable the cardholder entering his or her PIN. ▪ **N/A:** For HSMs, non-PEDs, SCRs, and SCRPs. A device cannot support both a physical keypad version and a touchscreen version under the same approval where both can be used for PIN entry. It may support a device that has both interfaces in connection with providing support for national or local disability laws.
Approved Components (PED, RAP, UPT)	**"Approved components"** contains, when relevant, the list of approved components that are part of the approved device, and which have successfully undergone a distinct evaluation. Each component is listed with its approval number. The use of a device with components—e.g., EPPs, card readers—that are different than that listed as an approved component for that device invalidates that device's approval. RAP devices may be listed as an approved component of one or more associated HSMs. For v4 and higher HSMs, the HSM must be validated to the Remote-Managed HSM requirements.

Feature and Applicability	Description
Functions Provided (EPP, HSM, Multi-tenant HSM, non-PED, PED, SCR, SCRP, UPT)	"**Functions provided**" denotes which of the following functions are supported by the device. One or more of the following may apply, depending on the implementation: ▪ **Card reader capabilities:** The device has components that can capture card data, such as magnetic-stripe reader (**MSR**) or ICC reader (**ICCR**) or Contactless (**CTLS**). ***Note:*** *Contactless readers are only considered compliant for P2PE usage if the device in question has been validated to SRED. Furthermore, some device approvals may have versions validated to SRED and some that are not. Where such a mix occurs, only devices using a firmware version designated for SRED are validated to meet the contactless reader Security Requirements. For devices with contactless readers using firmware that is not validated to SRED, the contactless readers are not validated to any Security Requirements.* ▪ **Display:** The device has an integrated display used for cardholder prompts—i.e., prompts for PIN entry—and possibly the presentation of other information. ▪ **SRED:** The device has met the applicable Secure Reading and Exchange of Data requirements. ▪ **OP:** The device has met the applicable Open Protocols requirements. ▪ **Remote Administration:** The HSM has been evaluated in conjunction with a remote administration solution and assessed against all requirements from the "Remote Administration" column in Appendix B of the HSM Security Requirements. Additionally, for v4 and higher HSMs, the HSM itself meets the Remote-Managed HSM Security Requirements as delineated in Appendix B of the HSM Security Requirements.

Feature and Applicability	Description
Additional Information	This field may be used to place any additional pertinent information. For example, when a vendor has changed the status of a device to end-of-life (EOL), as delineated in 5.4, "Approval-Listing Fee," and thus the device is no longer available for purchase except for maintenance purposes. Devices with EOL status are no longer supported by the vendor and no deltas are processed for those devices. The date and month of the EOL will be listed on the Website. ▪ **EOL** This will also be used for v2, v3, and v4 HSMs to delineate whether they are approved for restricted or unrestricted usage as delineated in the HSM Security Requirements: ▪ **Restricted** – Approval is valid only when deployed in Controlled Environments or more robust—e.g., Secure Environments—as defined in ISO 13491-2 and in the device's PCI HSM Security Policy. ▪ **Unrestricted** – Approval is valid in any environment. Devices supporting ISO PIN Block Format 4 (AES) will be noted here. For additional information on whether the MK/SK, DUKPT or Fixed Key methodologies are supported for AES PIN Blocks, see the Key Management section. POI v5 and higher devices supporting online PIN and HSM v4 and higher devices supporting PIN processing are required to support ISO PIN Block Format 4. ▪ **Supports ISO Format 4** (AES) PIN Blocks This field will also be used for notation for POI v6 and higher devices supporting Bluetooth and/or Wi-Fi that have been architected and evaluated to support unauthenticated wireless communications using those technologies. ▪ **Interface Isolation – Bluetooth** ▪ **Interface Isolation – Wi-Fi** In addition, v4 HSMs that meet additional criteria to support remote—e.g., non-console—administration for configuration and cryptographic key loading, will be noted here as "Remote-managed HSM." Requirements for Remote-managed HSMs are a subset of those for Multi-tenant HSMs ▪ **Remote-managed HSM** Devices must support key blocks using the ANSI X9.143 key-derivation methodology for TDES keys, and for AES keys, must support either the X9.143 methodology or the ISO 20038 methodology. In either case, equivalent methods can be used where subject to an independent expert review and where that review is publicly available. The link provided here is where a vendor who implements a proprietary method has had that method validated in accordance with PCI-prescribed criteria as equivalent. ▪ **Key Block Equivalency: <LINK>**

Feature and Applicability	Description
Device Form Factor	All security-relevant components (PIN pad, display, card reader(s)) of the device are shown in one or more pictures. At least one of the pictures must fulfill the requirement that the hardware version number must be shown on a label attached to the device. Note that for devices with multiple approved hardware versions, only one such illustration is necessary to facilitate purchasers of these devices recognizing how to determine the approved version(s).

Appendix B: Delta Evaluations – Scoping Guidance

B.1 Introduction

PCI SSC recognizes that vendors may need to make maintenance fixes to PTS validated devices that the vendor has already sold but still supports. In addition, vendors may wish to port updated versions of validated firmware that were assessed against newer versions of the Security Requirements to products for which the approval has expired. This may occur when customers wish to standardize their deployments against a given version of firmware and/or to add functionality to those devices.

This appendix provides guidance on whether changes made by vendors to a validated PTS Device (whether POI or HSM) are limited enough in scope such that it is permissible that said changes to the validated PTS Device may be assessed as a "delta" to the original validation. Any hardware changes to a PCI SSC-approved device that has been deployed must result in a new hardware version #. Any firmware changes to a PCI SSC-approved device must result in a new firmware version. Devices must undergo a delta evaluation when such changes are made.

B.2 What is a Delta Evaluation?

All initial evaluations under a major version—e.g., 1.x, 2.x, 3.x. 4.x, 5.x, 6.x, etc.—of the Security Requirements for a given product shall constitute a new evaluation and shall receive a new approval number.

Evaluation of deltas involve the PTS Lab assessing the changes based upon the most current major version of the Security Requirements used for the original evaluation and the most current Technical FAQ publication associated with those requirements. For example, if a device was originally assessed against PTS POI v6.0, any delta evaluation would have to be performed using the most current version of PTS v6.x and the last issued v6.x FAQs. Examples of deltas include:

- Revisions to existing firmware or hardware on previously approved devices to add, modify, or delete functionality[1].
  - Add or remove printer
  - Add NFC reader
  - Change in tamper-circuit functionality
- Adding EMV Level 1 to an existing approval.
- Maintenance fixes on devices that have expired approvals.
- Evaluation of a device for offline PIN entry where the existing approval is only for online PIN entry, or vice versa.
- The porting of a new set of firmware to an existing PCI SSC-approved device.

Delta evaluations are not permitted to take a product previously approved by PCI SSC under an earlier major version number of the PTS POI Standard—e.g., 5.x—to an approval under another major version number—e.g., 6.x.

[1] Some changes in functionality due to the number of changes or scope of changes may necessitate a full evaluation in lieu of a delta evaluation.

Technical FAQs need only be applied to any aspect of the device that is impacted by the changes made by the vendor. For example, if a vendor were to make changes to the hardware layout of the POI design but did not change the firmware in any way, any updated Technical FAQ entries that impact firmware only would not be applied to the delta evaluation. This is further delineated in the "Detailed Evaluation Process" section of the *PCI PTS Device Testing and Approval Guide.*

B.3 Determining Whether a Delta is Permissible

The potential for changes and their impacts cannot be identified in advance. Changes need to be assessed on a case-by-case basis. Vendors should contact one of the PTS Labs for guidance. PTS Labs shall consult with PCI SSC on an as-needed basis in advance of submitting a delta report to determine whether a set of changes is too great to be addressed under the delta process. The Laboratories will determine whether the change impacts security. In all cases, changes that impact security require an evaluation that must be presented in the delta report. At a minimum, for a given change type, all requirements identified in the tables below must be assessed for security impact. A rationale must be presented in the delta report for each change that is determined to not have a security impact.

B.3.1 Sample Impacts of Certain Changes

The following subsections itemize a non-exhaustive list of example changes that, taken individually, are permissible for consideration through the delta process. The inclusion of too many such changes, especially when considering a series of changes to the device's hardware, must be considered as a new device requiring a full evaluation to the latest version of the current PTS Standard.

B.3.2 Firmware Changes

In general, any and all changes made to the firmware that runs on a previously PCI SSC-approved PTS Device may be considered in a single delta evaluation except where the change is viewed as too pervasive, such as a change in the OS—e.g., changing from a proprietary to an open-based system. The following table identifies different types of firmware changes and the PTS requirements that, at a minimum, should be considered when assessing each type of change. PTS Labs evaluating such changes may rationalize the exclusion of any identified requirement or the inclusion of additional requirements based on their evaluation of the changes.

Table 8: Firmware Change Types and Impacted Requirements

Acceptable firmware changes that may be considered in a delta evaluation include, but are not limited to:

Firmware Change Types	Impacted Requirements					
	PTS POI Standard Version					
	v1.x	v2.x	v3.x	v4.x	v5.x	v6.x
Any firmware change	B3	B3	B3, F1, G1, H1, I1	B3, B20, F1	B3, B20, F1	B20, D2, E2
Changes in tamper management, for example, response, detection, and recovery	B1	B1	B1	B1	B1	B1
Error handling—i.e., buffer overflows	A5, B2	A3, B2	A3, B2	A3, B2	A2, B2	A3, D1
Amendments to external communications protocols	B2	B2	B2, F1, G1, H1, I1	B2, F1	B2, F1	D1, D2
Change to software/firmware update mechanisms	B3, B4	B3, B4	B3, B4, J4	B3, B4, B4.1, J4	B3, B4, B4.1, J4	E2, B2, B2.1,
New firmware/application authentication scheme	B4	B4	B4	B4, B4.1	B4, B4.1	B2, B2.1
Amendments to PIN-digit timeouts	B7, C3	B6, B10	B6, B10	B6, B10	B6, B10	B4, B8
Amendments to cryptographic functions; including PIN block formats and changes in random number process (for example, generation, seeding method, and algorithm)	B10, C2, C4, C6, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B4, B7, B11, B12, B21
Non-security changes to card-reader firmware	D4	A11, D4	A10, D4	A9, D4	A8, D4	A10, B21
Changes to sensitive service authentication mechanisms	B8, B9	B7, B8	B7, B8	B7, B8	B7, B8	B5, B6
Update key-loading methodology	C5	B11	B11, J4	B11, J4	B11, J4	B9, B2
Amendments to key management	C1, C5, C6, C7, C8	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B9, B12, B13, B18, A13
Change to key hierarchy	C1, C5, C7	B11, C1, D1	B11, C1, D1	B11, C1, D1	B11, C1, D1	B9, B18, A13
Amendments to key storage	C1, C5	B11, D1	B11, D1	B11, D1	B11, D1	B9, A13
New key types	C1, C5, C6	B11, B13, D1	B11, B13, D1	B11, B13 D1	B11, B13 D1	B9, B12, A13

Firmware Change Types	Impacted Requirements					
	PTS POI Standard Version					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**v6.x**
Amendments in PIN-length handling	C4, D4	B12, D4	B12, D4	B12, D4	B12, D4	B11, B21
User interface changes	B5, B6	B5, B15	B5, B15, F1 G1, H1, I1	B5, B15, F1	B5, B15, F1	B3, B14, D2
Updated PIN prompts	A7, B5, B6	A8, B5, B15	B5, B15, B16	B5, B15, B16	B5, B15, B16	B3, B14, B15
Addition, modification, or removal of SRED functionality ***Note:*** *SRED deltas on v2.x devices are not accepted.*	N/A	N/A	B17-19, K1-25	B17-19, K1-23	B17-19, K1-23	B1, B2, B2.1, B2.2, B4, B5, B6, B7, B9, B10, B12, B16, B16.1, B16.2, B17, B19, B22–B26, A2, A4, A6, A7, A10-A14, D1

B.3.3 Hardware Changes

Changes made by vendors to the hardware of previously PCI SSC-approved PTS Devices are permissible only if the scope of such changes is limited. The following table identifies different types of hardware changes and the PTS requirements that, at a minimum, should be considered when assessing each type of change. PTS Labs assessing such changes may rationalize the exclusion of any identified requirement or the inclusion of additional requirements based on their evaluation of the changes.

The inclusion of more than four (4) of the identified hardware change types as delineated in the table below in a single delta submission for a previously PCI SSC-approved PTS POI Device may effectively represent a new device that should be subjected to its own full evaluation against the latest version of the current PTS Standard. Candidates for delta submissions that surpass this threshold which, in the opinion of the PTS Lab, represent a minor change to the approved PTS POI Device, must be presented to PCI SSC in advance of completing the evaluation to determine whether the scope of change is too great. Reports submitted with changes in excess of four change types will be rejected unless PCI SSC has pre-approved the submission. Regardless of pre-approval, PCI SSC may, upon review of the report, determine the changes too excessive for a delta evaluation and require a full evaluation resulting in a new and separate device listing.

It is not acceptable to put forward a series of delta submissions with hardware changes as an attempt to work around this threshold. If delta submissions with hardware changes are received within three months of the approval of the reference device, sufficient information must accompany the submission to justify the need for the change and why it wasn't included as part of the previously PCI SSC-approved submission. In all cases, cumulative changes will be considered when assessing the propriety of any specific delta request.

For example, a vendor makes a change to the tamper grids and signal routing on six PCBs within a device. According to the delta scoping guidance, the inclusion of four or more hardware change types in a single delta submission for a previously PCI SSC-approved PTS POI Device may effectively represent a new device that should be subject to its own full evaluation against the latest version of the current PTS Standard. In this example, this does not count as six changes but rather counts as a single change since they are all of the same change "type." This meets the criteria for a delta.

A device submitted with internal hardware changes sufficient to require a new evaluation—but with no external changes—cannot be submitted as a delta, even though the external appearance is identical. The degree of changes made internally requires that the device receive a full evaluation against the currently available requirements version for use in new evaluations. If the evaluation is successful, it will result in a new approval number. Furthermore, while the new device will have a different hardware version than the existing device, it is also required to have a new model name/number. This is to prevent confusion in the market, especially if issues arise subsequent to deployment impacting only one of the approvals but not the other(s).

Replacing a PCB does not count as a single change. All changes related to the PCB change need to be taken into account. For example, changing the PCB re-routes the tamper grid and signals. That would count as one. Moving a processor would also count as a change and needs to be assessed accordingly. Any other security-relevant changes resulting from the change in the PCB would also add toward the change count.

Any change made to the hardware of a PCI SSC-approved PTS device, even to the non-security related components, has the potential to impact the security of the device directly or indirectly. As such, any delta evaluation that includes modifications to the approved device's hardware—even the circuitry not related to the security functions of the device—must, at a minimum, be reviewed by the PTS Lab with respect to the potential impact. For example, for POI devices the following requirements of the applicable version of the Security Requirements against which the evaluation is being performed must be reviewed:

- V1.x: Requirements A1, A2, A3, & C1
- V2.x: Requirements A1 & A7
- V3.x: Requirements A1 & A7
- V4.x: Requirements A1, A6, B2, & B20
- V5.x: Requirements A1, A5, B2, & B20
- V6.x: Requirements A1, A2, A6, A7, B20, & D2

Table 9: Acceptable Hardware Changes

Acceptable hardware changes that may be considered in a delta evaluation include, but are not limited to:

Hardware Change Types	Impacted Requirements					
	PTS POI Standard Version					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Any hardware change[2]	A1, A2, A3, C1	A1, A7	A1, A7	A1, A6, B2, B20	A1, A5, B2, B20	A1, A2, A6, A7, B20, D2
Changes in casing plastics—e.g., cover-opening dimensions, areas that permit internal access—or output-only displays. Amended devices must remain consistent to the device's original form factor and visible characteristics.[3]	A4, A7, A9–A11, D1–D4	A2, A6, A8–A11, D1–D4	A2, A6, A8–A11, B16, D1–D4, K1–K3	A5, A7–A9, A11, B16, D1–D4 K1–K3	A4, A6–A8, A10, B16, D1–D4 K1–K3	A5, A7-A9, B5, B15, B21, A13, A14, A11, A12, A6
Modification to tamper/removal switches—e.g., changes to materials, performance, location, circuitry, tamper response, etc.—or tamper-resistance/evidence features.	A5, D1	A2, A3, A11, D1	A2, A3, A10, D1	A2, A9, D1	A2, A8, D1	A3, A10, A13
Modifications or replacement of any processor used by the device. [4]	A5, A6, A7, A9, B1-B10, C2-C8, D4	A3, A4, A6, A8, B1-B15, C1, D4	A3, A4, A6, A8, A11, B1-B19, C1, D4	A3, A4, A5, A7, A10, B2–B19, C1, D4	A2, A3, A4, A6, A9, B2–B19, C1, D4	A3, A4, A5, A6, A7, B2-B19, B21

[2] This item is not to be included in the count of changes when determining whether the number of changes in a single delta submission is within the acceptable range of four (4). Any hardware change requires a change in hardware version number done in accordance with Appendix A.

[3] "Visible characteristics" refers to the gross geometry or "look-and-feel" of the device including its physical dimensions. "Form factor" refers to relative and absolute dimensions of the device. Relative dimensions would include the ratio of length to width, etc. Absolute dimensions are the individual dimensions themselves—e.g., length, width, thickness, depth, etc. Changes affecting *form factor* or *visible characteristics* are allowed for delta evaluations provided the change(s) in relative and absolute dimensions does not exceed plus or minus ten-percent of the existing dimensions. For example, the addition or removal of a printer, LCD display, bar code reader, or extended battery compartment that changes the depth of the device is acceptable so long as it does not change the security of the device and does not change the *form factor* by more than 10% in any dimension. However, even as a delta, it will require a model name change that can be co-listed with the original listing.

[4] Each processor modification or replacement counts as a separate hardware change—e.g., if both the secure processor and application processor are modified it would count as two hardware changes.

Hardware Change Types	Impacted Requirements					
	PTS POI Standard Version					
	v1.x	**v2.x**	**v3.x**	**v4.x**	**v5.x**	**V6.x**
Changes to user interfaces that could be used for PIN entry—e.g., touch screens, keypad membranes, buttons, etc., but excluding modifications of function keys.	A5, A7, A9, D1	A2, A6, A8, A9, A11, D1	A2, A6, A8-A10, B16, D1	A5, A7-A9, A11, B16, D1	A4, A6-A8, A10, B16, D1	A5, A8-A10, B5, B15, A13
Replacement or addition of any one reader.[5]	D1-4	A10, A11, D1-4	A10, D1-D4, K1, K2	A9, D1-D4 K1-K2	A8, D1-D4 K1-K2	A10, A11-A14, B21
Modifications to communications circuitry.	A5, B2, D1	A2, A3, B2, D1	A2, A3, B2, D1, F1, G1, H1, I1	A3, B2, D1, F1	A2, B2, D1, F1	A3, A13, D1, D2
Modifications to power circuitry.	A5	A3	A3	A3	A2	A3
Changes in PCB or FPCB stack-up—e.g., adding or removing layers, shuffling layers—and/or change in PCB geometry—e.g., board outline, thickness.	A5-A7, A9, B2, B8, D1, D4	A3, A4, A6, A8, A11, B2, B7, D1, D4	A3, A4, A6, A8, A10, B2, B7, B16, D1, D4, K3	A2-A5, A7, A9, B7, B16, D1, D4, F1, K3, L1, L3	A2-A4, A6, A8, B7, B16, D1, D4, F1, K3, L1, L3	A3, A5, A7, A8, A10, A13, B5, B15, B21, D12, D13, E1, E4
Modifications to major components (other than communications or power) of the PCB circuitry—e.g., audio circuitry, heater circuitry, printer, display etc.,—as well as addition or removal of a PCB (or FPCB). [6]	A5, A8	A3, A5	A3, A5	A3, A11	A2, A10	A3, B5

[5] Each reader change counts as a separate hardware change—e.g., if both the MSR and ICCR are changed, that counts as two separate hardware changes. However, a change involving a hybrid reader counts as only one hardware change.

[6] This excludes rerouting of circuits.

B.4 Engaging a PTS Lab to Perform a Delta Evaluation

Vendors may select a different PTS Lab to perform a delta evaluation other than the PTS Lab used to perform the initial evaluation or prior delta evaluation. However, the subsequent PTS Lab ("Delta Lab") is free to determine the level of reliance it wishes to place upon the prior PTS Lab's work and will be responsible for any claims of compliance which are generated through the delta review; and this may result in additional work than would otherwise be necessary. For POI version 3 (version 2 for HSMs) or higher reports, the Delta Lab shall have access to the prior PTS Lab's report(s), including any delta or OEM component reports subsequent to the original evaluation. If those reports are not available, the Delta Lab either shall decline the engagement or must complete a full evaluation of the device.

B.5 Delta Documentation Requirements

B.5.1 Reporting Guidance for PTS Vendors

All changes made to PCI SSC-approved PTS Devices must be disclosed by the PTS vendor. It is recommended PTS vendors submit a Change Analysis document to the PTS Lab that contains the following information at a minimum:

- Name of the approved PTS Device;
- New hardware, firmware, and application version numbers, as applicable, to be assessed;
- Details of the currently approved PTS Device on the Approved Device List that is being used as a reference for the evaluation;
- Details of the PTS Lab that performed the original evaluation on the device, and information on any subsequent delta evaluations performed on that device since the original approval;
- Description of the change;
- Description of why the change is necessary;
- Description of how the change functions;
- Explanation of how and why PTS Security Requirements are impacted;
- Description of testing performed by the vendor to validate how PTS Security Requirements are impacted; and
- Description of how the identification (versioning) of the change fits into vendor's configuration-control methodology.

B.5.2 Reporting Requirements for PTS Labs

Delta evaluation reports must present all relevant information on changes and changes' evaluation, equivalent to the levels of detail specified in DTRs. PTS Labs must provide the following documentation with each delta submission:

- The number of any identified hardware change types;
- A high-level description clearly defining all of the changes that have been made to the approved PTS Device;
- Citations of:
  - The reference approval report and any subsequent delta submissions upon which the current delta submission is based, and

  - Any supporting documentation used to substantiate the findings represented in the delta submission;
- A table that depicts the following information about every change embodied in the update to the approved PTS Device from the previously approved configuration:
  - A description of the change;
  - Identification of the amended configuration item or items (system files or hardware components) impacted by the change;
  - A high-level evaluation of the security impact of the change;
  - Identification of the PTS Security Requirements that are impacted by the change (including requirements for which the previous responses remain accurate without change); and
  - A high-level description of the completed testing, if any, used to validate the evaluation;
- Updated responses to the affected PTS Security Requirements that clearly depict any changes that are necessary to the reference evaluations.

B.6 Applicability of Technical FAQs During Delta Evaluations

Technical FAQs are updated on a regular basis to not only add clarification to requirements in order to provide a consistent and level playing field in the applications of those requirements but may also address new security threats that have arisen. As such, Technical FAQs are generally effective immediately upon publication.

The intent is not to cause a device in evaluation to fail due to the publication of such FAQs subsequent to the approval of that device. This may, however, be necessary if known exploits exist that significantly change the threat environment for the device from when it was originally evaluated. Unless one or more such exploits exist, a product currently in evaluation will generally not be subject to new FAQs issued during the product's evaluation. This does not exempt a product from the applicability of the FAQ if the product must be reworked and resubmitted at a later date because of other issues that cause it to fail the evaluation.

Devices undergoing delta evaluations must take into account the current FAQs of the associated major version of Security Requirements only for the security requirement(s) that are impacted by the delta change. For example, if a change impacts compliance with Requirements B1 and B4, only the current FAQs associated with B1 and B4 must be considered as part of the delta.

Furthermore, it is not sufficient for the Lab to determine that the change does not lessen the security of the device. Due to the evolution of threats and attack techniques from the time of the original evaluation (which may have occurred many years earlier), the Lab must determine that the device still meets the relevant Security Requirements impacted by the change, given the changes in attack vectors. This is because, whether deltas are done to enhance or fix functionality or for other purposes, the end result is to extend the life of the device in the marketplace.

In all cases, the PTS Lab performing the evaluation must advise PCI SSC of the circumstances, and PCI SSC will make the final decision based upon the circumstances. Additionally, for both new and delta evaluations, the PTS Lab will also state in their submission the version of the Security Requirements used in the evaluations, as well as the publication date of the technical FAQs used.

B.7 Considerations for Updated Components in Integrated Terminals

Vendors with PCI SSC-approved PTS Devices that integrate other PTS Program-approved OEM components (such as unattended payment terminals) may seek delta evaluations on such devices for changes that occur to the embedded OEM components, including replacement of any given OEM component with a different mode—e.g., a separately approved OEM ICCR produced by one vendor is replaced in the final form factor of the integrated terminal or UPT with a different model, even if from a different vendor. This allowance applies as long as the vendor continues to have control over the final assembly and manufacture of the integrated terminal or UPT.

Changes that occur in the final form factor itself—e.g., the housing, because of the complexity of integration—must undergo testing as a new evaluation against a version of the Security Requirements that has not been retired from use for new evaluations.

In all cases, though, any Security Requirements impacted will be assessed, including those not previously applicable—e.g., if the new casing introduces additional cardholder-interface devices not present in the original evaluation.

Appendix C: PTS Administrative Change Request

Administrative changes impacting a PCI SSC-approved PTS Device, PTS vendor business name and/or address, or contact details must be disclosed in this *Administrative Change* document. Vendors must complete each section then submit the document to a PCI-Recognized Laboratory. The Lab must then submit the required supporting documentation via an Administrative Change to PCI SSC for review. Changes that include new images must have the images submitted via a delta submission.

PTS Vendor Company Details			
Name of Company		Submission Date	
Name of Individual Requesting Change		E-mail address:	
Job Title of Individual Requesting Change		Role (Primary Business, Secondary Business, Billing, Technical)	

Description of PTS Vendor Change(s)		
Type of Change (check all that apply)	☐ Business Name ☐ Business Website ☐ Mailing Address ☐ Billing Address ☐ Device Model Name(s)	☐ Billing Contact Name/Address ☐ Technical Contact Name/Address ☐ Primary Business Contact Name/Address ☐ Secondary Business Contact Name/Address
Briefly describe reason for change(s)		

Revised Company Details			
New Business Name		New Website	
New Mailing Address			
New Billing Address			

Device Model(s)			
PTS Approval Number	**Model Name**	**New Model Details**	
		New Model Name	Image included *
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

** At "New Device Model Images" on last page.*

Primary Business Contact			
Contact Name		Business Title	
Contact E-mail		Contact Phone	

Secondary Business Contact			
Contact Name		Business Title	
Contact E-mail		Contact Phone	

Billing Contact *(invoices will be sent to this individual/email address)*			
Contact Name		Business Title	
Contact E-mail		Contact Phone	

Technical Contact			
Contact Name		Business Title	
Contact E-mail		Contact Phone	

Supporting Documentation Required

	Administrative Change (this form)	Security Policy	Vendor Release Agreement	Device Images*
Revised Company Details Changes	**X**	**X**	**X**	**X**
Contact Name Changes	**X**			
Device Model Name Changes	**X**	**X**		**X**

Appendix D: Attestation of Validation

Instructions for Submission

The PTS vendor must complete this document as a declaration of the firmware's validation status with the PCI PTS POI or HSM Security Requirements, as applicable. Vendors or other third parties licensing PCI SSC-approved products from other vendors to market or distribute under their own names are not required to complete this attestation where the licenses do not make any changes to the firmware, except when making updates based upon the same changes the OEM vendor has made to their own product upon which the licensed product is based.

The PTS vendor should complete all applicable sections and submit this document along with copies of all required validation documentation to PCIPTS@pcisecuritystandards.org per PCI SSC's instructions for report submission as described in the *PTS Device Testing and Approval Program Guide*.

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 unexpired HSM or POI approval as of the prior year ending 31 December, indicate hardware and firmware submission status as either:

A: No modifications requiring a delta evaluation have been made to the hardware or firmware version.

B: All hardware and firmware changes have been assessed by a PTS Lab in a report submitted to PCI SSC, including those hardware or firmware versions noted as using a validated wildcard versioning methodology. This includes for POI devices all vulnerabilities identified by the vendor in each of the protocols and interfaces defined in POI security requirement D1 as evidenced by the vulnerability assessment process enumerated under E10 through E12 of the POI DTRs.

For all POI devices, the vendor shall provide evidentiary materials that an auditable record of an ongoing vulnerability assessment process exists by providing a copy of the vendor's sign-off form specified in POI Requirement E10 for the prior year ending 31 December.

PTS Approval Number	Approval Expiry Date	Model Name	Firmware Version	Hardware Version	Firmware submission status for the 12 months ending December 31 of the prior year	
					A	B
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐
					☐	☐

Part 3. PTS Vendor Acknowledgment	
Signature of PTS Vendor Executive Officer ↑	*Date ↑*
PTS Vendor Executive Officer Name ↑	*Title ↑*
PTS Vendor Company Represented ↑	

Appendix E: 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 Approved Device List;

B: All hardware and firmware changes have been assessed by a PTS Lab in a report submitted to PCI SSC, 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 ↑	