



Payment Card Industry (PCI) **PIN Transaction Security (PTS)**

Device Testing and Approval Program Guide

Version 1.1

October 2011

Document Changes

Date	Version	Description
October 2011	1.1	Add approval classes for encrypting card readers and non-PEDs

Table of Contents

Document Changes	i
Introduction	1
Related Publications	1
Updates to Documents and Security Requirements.....	3
About This Document	4
About the PCI Security Standards Council.....	5
Payment Brand Rules.....	5
Testing and Approval Process Description	6
Overview	6
Prior to Testing (POI devices only)	6
The Modular approach.....	7
Testing Process	7
Figure 1: PTS Device Testing Inquiry Flow Chart	9
Figure 2: PTS Device Approval Flow Chart	10
Figure 3: PTS Device Change Request and Renewal Flow Chart	11
Detailed Evaluation Process	12
Required Documentation and Materials	12
Preparation for Testing.....	14
Laboratory Services	14
PCI-Recognized Laboratories.....	14
Fees	14
Requirements for Testing	15
Test Dates.....	15
Testing Timeframes	15
Test Cycle Definition	16
Technical Support throughout Testing.....	16
Approval Process.....	17
Release Agreement and Delivery of Report	17
Roles and Responsibilities.....	17
Issuance of Approval	17
Expiry of Approval.....	18
Changes to a Previously Approved PTS Device.....	19
Maintaining Approval	19
Boundary of Approval	20
Notification Following a Security Breach or Compromise	21
Notification and Timing	21
Notification Format.....	21
Notification Details	21
Actions following a Security Breach or Compromise.....	22
Withdrawal of Approval.....	22
Legal Terms and Conditions.....	23
Glossary of Terms and Acronyms	24

Appendix A: Device Listing on PCI SSC Website	26
Point of Interaction (POI)	26
Hardware Security Module (HSM)	26
Device Identifier	27
Table 1: Example of a Device Identifier (four components)	27
Hardware #	28
Table 2: Examples on the Use of Hardware #s.....	28
Approval Number.....	29
Product Type.....	29
Approval Class.....	29
Table 3: Approval Class Descriptions	29
Version.....	31
Expiry Date	31
Specific Features per Approval Class	32
Table 4: Specific Features.....	32

Introduction

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

Related Publications

In addition to this Program Guide (describing the testing and approval process) the Payment Card Industry (PCI) Security Standards Council (SSC) PIN Transaction Security (PTS) framework includes the following documents.

Note: These documents are routinely updated and reaffirmed. The current versions should be referenced when using these requirements. The most current standards will be available at www.pcisecuritystandards.org.

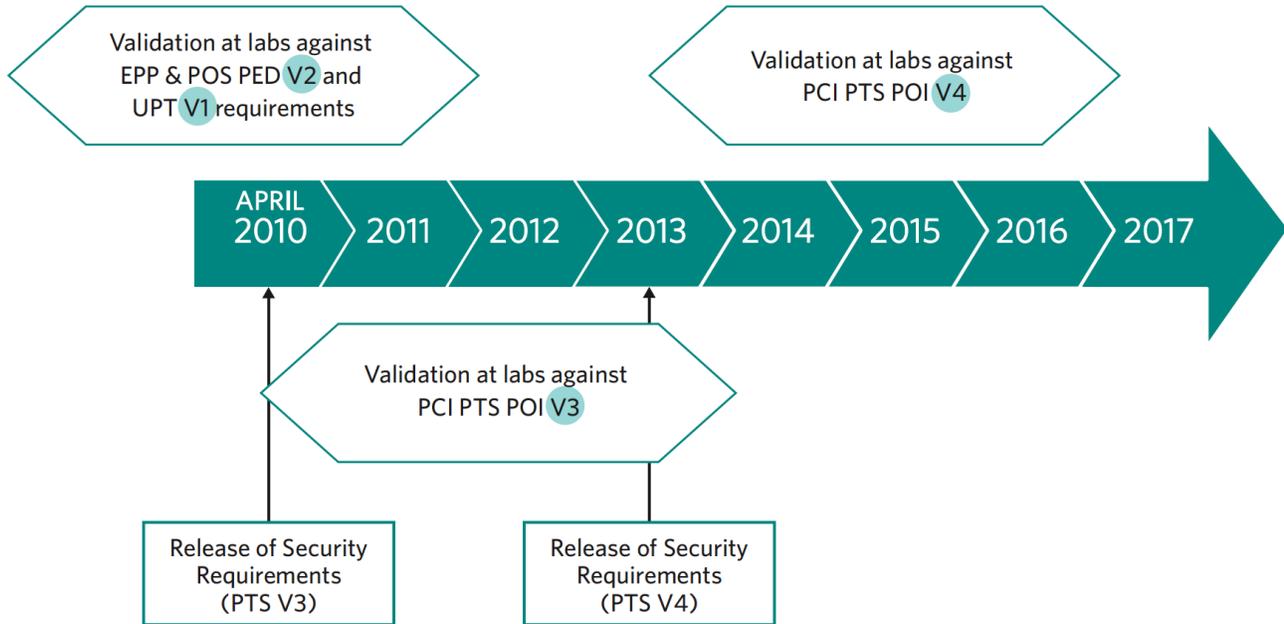
Document Name	Description
Security Requirements	
<ul style="list-style-type: none"> ▪ <i>PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements - v3.x</i> ▪ <i>Encrypting PIN Pad (EPP) Security Requirements- v2.1</i> ▪ <i>POS PIN Entry Device Security Requirements- v2.1</i> ▪ <i>Hardware Security Module (HSM) Security Requirements, v1.0</i> ▪ <i>Unattended Payment Terminal (UPT) Security Requirements - v1.0</i> 	<p>Contain the physical and logical security requirements as well as device management requirements for activity prior to initial key loading.</p> <p>Provide the forms to be used by laboratories and vendors.</p>
FAQs	
<ul style="list-style-type: none"> ▪ <i>PIN Entry Device Security Requirements: Frequently Asked Questions</i> 	<p>General frequently asked questions</p>
<ul style="list-style-type: none"> ▪ <i>PTS POI Security Requirements Technical FAQs for use with Version 3.0</i> ▪ <i>POS PED Security Requirements and EPP Security Requirements Technical FAQs for use with Version 2.0</i> 	<p>Provide additional and timely clarifications to the application of the Security Requirements. The FAQs are an integral part of those requirements and shall be fully considered during the evaluation process.</p>
Evaluation Vendor Questionnaires	
<ul style="list-style-type: none"> ▪ <i>PIN Transaction Security (PTS) Point of Interaction (POI) Modular Evaluation Vendor Questionnaire - v3.x</i> ▪ <i>PIN Transaction Security Encrypting PIN Pad (EPP) Evaluation Vendor Questionnaire - v2.1</i> ▪ <i>POS PIN Entry Device (PED) Evaluation Vendor Questionnaire - v2.1</i> ▪ <i>Hardware Security Module (HSM) Evaluation Vendor Questionnaire - v1.0</i> ▪ <i>Unattended Payment Terminal (UPT) Evaluation Vendor Questionnaire - v1.0</i> 	<p>Solicit additional information from vendors to support their claims of the conformity of their devices to those requirements.</p>

Document Name	Description
Derived Test Requirements	
<ul style="list-style-type: none"> ▪ <i>PIN Transaction Security (PTS) Point of Interaction (POI) Derived Test Requirements - v3.x</i> ▪ <i>Encrypting PIN PAD (EPP) Derived Test Requirements - v2.1</i> ▪ <i>POS PIN Entry Device Derived Test Requirements - v2.1</i> ▪ <i>Hardware Security Module (HSM) Derived Test Requirements - v1.0</i> 	Provide specific direction to vendors on methods the test laboratories may apply when testing against the requirements
Recognized Laboratories List	
<i>Payment Card Industry (PCI) Recognized Laboratories</i>	Currently recognized laboratories for PTS device testing.
Vendor Release Agreement	
<i>PIN Transaction Security Device Security Evaluation Testing Program Vendor Release Agreement</i>	Contains the terms and conditions that govern the exchange of information between vendors and the PCI SSC
Approved Terminal Models List	
<i>Approved PIN Transaction Security Devices</i>	List of PCI SSC Approved PIN Transaction Security Devices

The documents above described are available in the “PIN Transaction Security” section of the PCI SSC website – www.pcisecuritystandards.org. Earlier versions of the documents are available can be found in the PIN Transaction Security Document Archive of the same website.

Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, it is necessary to regularly review, update, and improve the security requirements used to evaluate POI devices and hardware security modules, collectively referred to as “payment security devices.” As such, PCI SSC has agreed that all relevant security requirements and associated test requirements will be normally updated every three years. The following diagram describes the three-year cycle of Security Requirements v3, its predecessors, and successor v4.



PCI SSC reserves the right to change, amend, or withdraw security requirements at any time. If such a change is required, PCI SSC will endeavor to work closely with customers¹ and vendors to help reduce the impact of any changes.

¹ Customers are financial institutions that:

- a) Offer payment cards for one or more of the participating payment brands (issuers);
- b) Accept such payment cards for cash disbursement and directly or indirectly enter the resulting transaction receipt into interchange (acquirers); or
- c) Offer financial services to merchants or authorized third parties who accept such payment cards for merchandise, services, or cash disbursement, and directly or indirectly enter the resulting transaction receipt into interchange (acquirers).

In accordance with any mandates issued by the participating payment brands, customers should use the testing and approval results from PCI SSC when making decisions about purchasing devices that have been approved within the PCI PTS framework.

About This Document

The *Payment Card Industry PIN Transaction Security (PTS) Device Testing and Approval Program Guide* provides information for vendors regarding the process of evaluation and approval by PCI SSC of payment security devices, and reflects an alignment of the participating card payment brands to a standard set of:

- Point of interaction (POI) and hardware security module (HSM) security requirements,
- Testing methodologies, and
- Approval processes.

Throughout this document:

- “PCI participants” or “PCI payment brand participants” means any entity then-currently admitted as a member of the Council in accordance with the Delaware Limited Liability Company Act. The PCI participants as of the date hereof are American Express Travel Related Services Company, Inc., DFS Services LLC (Discover), JCB Advanced Technologies, Inc., MasterCard International Incorporated, and Visa Holdings, Inc.
- “PCI SSC,” “PCI,” or “Council” refers to the PCI Security Standards Council, LLC, a Delaware limited liability company, which consists of the payment card brands referenced above under “PCI participants.”
- “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 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.
- “PIN Transaction Security” refers to the framework within PCI standards and requirements that deals with the evaluation and approval of payment security devices.

About the PCI Security Standards Council

The Payment Card Industry (PCI) Security Standards Council has established the PIN Transaction Security framework, to address the security evaluation and approval of payment security devices.

This *Payment Card Industry PIN Transaction Security Device Testing and Approval Program Guide* reflects an alignment with the participating payment brands to a standard set of:

- Security requirements,
- Testing methodologies, and
- Approval processes

Note:

Approvals are granted directly through PCI SSC and are coordinated by the participating PCI payment brands through the PCI PTS Program process.

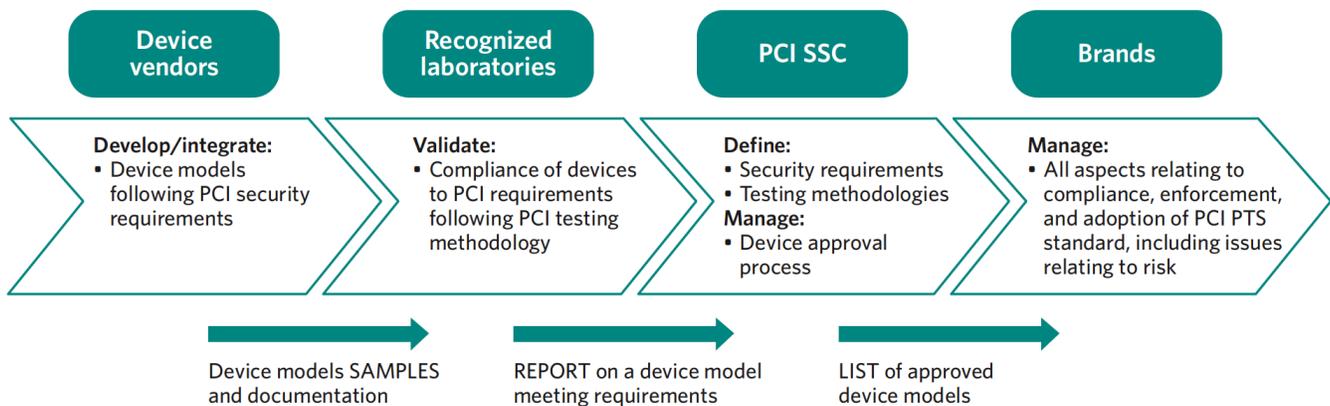
All devices submitted for security evaluations and approval have been evaluated against the applicable aligned Payment Card Industry (PCI) PTS Security Requirements. The PCI Approval Lists provide a full list of payment security devices recognized as meeting PCI PTS Requirements.

This collaborative effort ensures that all payment security devices will be evaluated under a common process offering a high degree of assurance. This arrangement is intended to improve the overall security for cardholder and other sensitive data by removing conflicting requirements. All stakeholders in the payments value chain benefit from the aligned requirements:

- Customers benefit from a broader selection of secure devices.
- Merchants, financial institutions, processors, and other third parties are assured that they will be using products that have met the required level of assurance.
- Vendors are able to reduce the “time to market” for new devices, as they will only be required to complete a single security evaluation and single approval process.

Payment Brand Rules

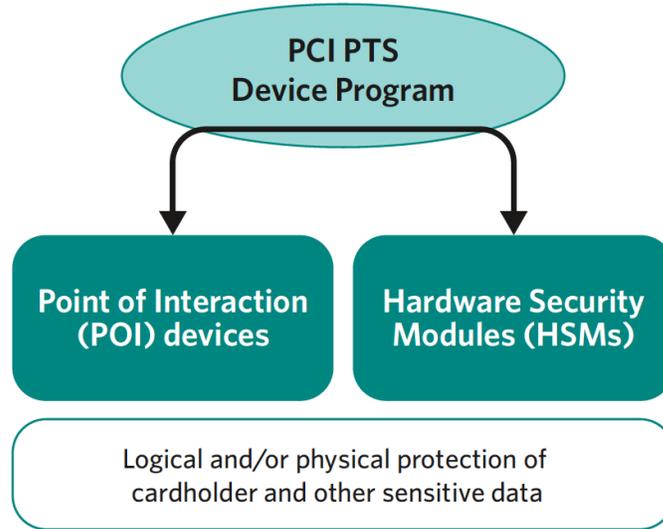
All aspects relating to compliance, enforcement, and adoption of these standards, including all issues relating to risk, are the responsibility of the individual payment card brands. The following picture provides a high-level description of the device security chain.



Testing and Approval Process Description

Overview

The PCI SCC PTS security approval framework addresses the logical and/or 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 the PCI SSC may contact one of the PCI-recognized laboratories and complete the appropriate PCI forms (included in the *PCI PTS Security Requirements* and the *PCI Vendor Questionnaires* themselves). The vendor will then submit the device, together with any additional documentation required by the laboratory, for evaluation and compliance validation against the PCI PTS Security Requirements. Upon completion of the evaluation, PCI SSC will review the evaluation report. When the device model meets the PCI requirements, an approval letter will be issued confirming successful completion of the process. Once the payment security device model is approved, it will be listed on the PCI PTS website.

Prior to Testing (POI devices only)

- PCI SSC recommends that the POI device receive EMV Level 1 approval first, if applicable, and then PCI 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 types of PIN-entry options, online and offline, 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.

The Modular approach

The PCI PTS modular 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 approval of product types; and the maintenance of existing approvals (changes in security components, etc.).

The PCI PTS modular approach supports the submission of devices in accordance with the product types and approval classes defined in *Appendix A*.

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

Requirements and Evaluation Module Name	Description
POI Device Core Requirements	Core logical and physical requirements of PIN acceptance devices
Device Integration Requirements	Considers how the device is produced, controlled, transported, stored, and used throughout its life cycle.
Open Protocols (OP)	The interface of POI terminals to open networks using open protocols
Secure Reading and Exchange of Data (SRED)	To support secure encryption of account data in the POI
Device Management Security Requirements	Considers how the device is produced, controlled, transported, stored, and used throughout its life cycle.

The first two modules roughly correspond to previous versions of the PCI PED, EPP, and UPT Security Requirements manuals.

Testing Process

Payment security devices are evaluated using the requirements embodied in the *PCI PTS POI Modular Security Requirements* or *PCI Hardware Security Module Requirements* manual (“HSM manual”), 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 via information and the required payment security device samples.

Any product that incorporates separate modules, such as EPPs, card readers, etc., must complete the integration requirements. Products are not required to support open protocols or the secure reading and exchange of data; however, if they do, then those modules are mandatory for evaluation and approval.

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

The laboratory does not evaluate the payment security devices against the Device Management Requirements as specified in the *PCI PTS POI Modular Security Requirements* or *PCI HSM Security Requirements*; nevertheless these are requirements, and the information is required as part of the approval process. Such conformance may be separately evaluated by PCI SSC at their discretion.

Testing and Approval Process Illustration

The table below and the charts on the following pages outline and illustrate the 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 test laboratory to initiate testing	Preparation for Testing	Figure 2
Sign NDA and release agreement	Approval Process	Figure 2
Submit documentation and materials	Requirements for Testing	Figure 2
Respond to inquiries from test 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

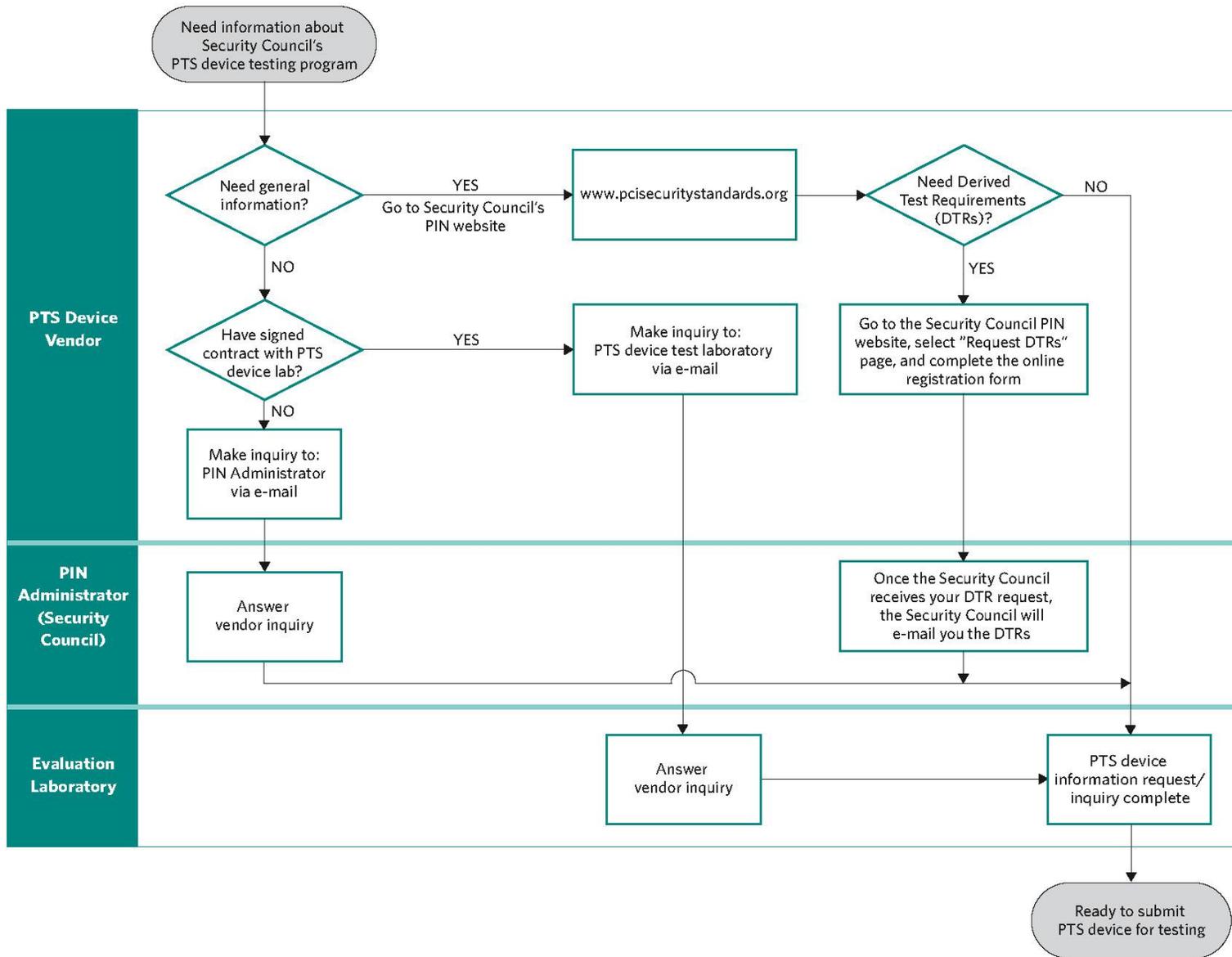
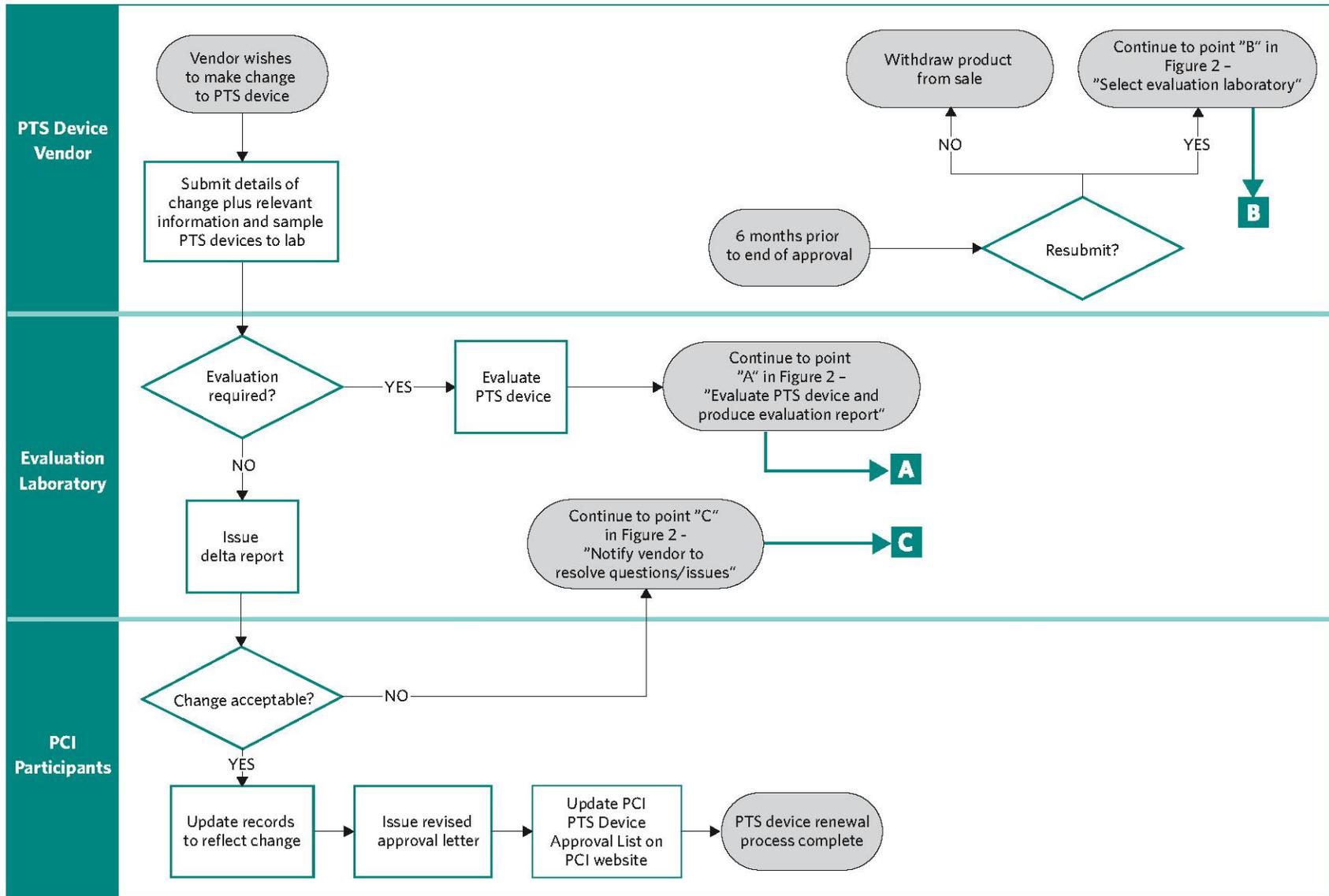


Figure 3: PTS Device Change Request and Renewal Flow Chart



Detailed Evaluation Process

Payment security devices will be evaluated against the *PCI PTS POI Modular Security Requirements* or the *Payment Card Industry Hardware Security Module Security Requirements* manual. The laboratory will evaluate the vendor's responses in those sections by having the vendor provide additional evidence of conformance to the requirements—via information and 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, the payment security device is approved and an Approval Letter will be issued to the vendor. The PTS device is then posted as a “PCI approved” payment security device on www.pcisecuritystandards.org.

The Technical FAQs are an integral part of the evaluation process. Technical FAQs are identified by major version of security requirements, e.g., 1.x, 2.x, 3.x. Each Technical FAQ version is specific to the corresponding major version of security requirements. For example, Technical FAQs version 3 is specific to security requirements version 3.x and only security requirements version 3.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), their applicability may be deferred for devices which are under evaluation at the time of publication.

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 taken into account as part of the delta.

Required Documentation and Materials

All information and documents relevant to the PCI PTS Testing and Approval Program can be downloaded from www.pcisecuritystandards.org. All completed forms and questionnaires related to payment security device evaluation must be delivered to a PCI-recognized testing 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 payment security device test laboratory include as applicable for device approval class:

1. Completed appropriate *PCI Security Requirements* forms for device
2. Completed appropriate *PCI Evaluation Vendor Questionnaire* for device
3. Three (3) working POI devices (for HSMs, consult with the laboratory) with operator's manual or instructions
4. The necessary hardware and software accessories to perform simulated PIN-based payment transactions (for HSMs, consult with the laboratory)
5. 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 key pad) must be described. (An API manual is an example of documentation that could fulfill this requirement.)
6. 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

7. Instructions and accessories (such as key loaders) that will allow the test 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
8. Additional documentation—such as block diagrams, schematics, and flowcharts—that will aid in the payment security device evaluation. (The laboratory may request additional evaluation material when necessary.)

Applicable to POI devices only:

Following a successful evaluation, the vendor must provide to MasterCard, on behalf of all of the PCI participants, two (2) terminals containing the same keys and applications as those supplied to the PCI-recognized laboratory. MasterCard will securely retain these terminals, and may use them to assess vulnerability to new attack techniques. Also, if a terminal of that model is ever compromised in the field, the retained samples may be used to investigate any compromise or security breach. Devices should be sent to:

Attn: MasterCard Analysis Laboratory (MCAL)
MasterCard Worldwide
St Andrews House
Kelvin Close
Birchwood
Warrington
Cheshire
UK
WA3 7PB

Preparation for Testing

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 PCI 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 assessment on a vendor's hardware
- Guidance on bringing a vendor's payment security devices into compliance with the PCI requirements if areas of non-compliance are identified during the evaluation.

Vendors are encouraged to contact a PCI-recognized laboratory directly in regards to the above services and any fees associated with them. However, the laboratories **cannot** offer any advice on the actual design of the POI device or HSM.

PCI-Recognized Laboratories

PCI SSC currently recognizes a series of laboratories for PTS device testing. The current list of recognized PTS test labs may be found at the PCI SCC website, in the "PCI PTS" section.

Fees

All testing-related fees and dates are negotiated between the vendor and laboratory, and the vendor pays all 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 evaluation fees directly to the laboratory.

Vendors are assessed a \$2,000 fee for every new evaluation report received. In addition, vendors will be assessed an annual listing or maintenance fee of \$1,000 for each existing PCI approval.

Vendors or other third parties licensing approved products from other vendors to market or distribute under their own names are not required to pay a new evaluation fee if the only change is to the name plate. If firmware or other hardware changes are made that require a PCI-recognized test laboratory to evaluate the changes for potential security impact, then the licensee shall be required to pay the new evaluation fee. Additional considerations for licensing products are stipulated in the *PCI PTS POI Security Requirements Technical FAQs*.

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.

The fee for new evaluations will be a pass-through fee from the applicable test laboratory to the vendor. The test laboratory will provide the monies to PCI SSC and recover such fees as part of the evaluation fee. The fee will be billed quarterly, for all new evaluations submitted by the lab for the preceding three months. Vendors shall not be billed for modifications of hardware or firmware in existing PCI approvals, termed "delta" approvals.

All initial evaluations under a major version (e.g., 2.x, 3.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., 2.x—to an approval under another major version number, e.g., 3.x.

The approval-listing fee will be billed annually by PCI SSC to vendors for all PCI approvals existing for that vendor on the billing date. The billing date shall be set as May 1 of every year, as PCI approvals shall expire April 30 of any given year, depending on the device type and requirements version approved under. For example, EPPs and attended POS PEDs approved under Version 1 of the respective requirements shall expire with April 30, 2014; Version 2 EPPs and attended POS PEDs shall expire April 30, 2017, and so forth—i.e., on May 1 vendors shall be billed per PCI approval for each approval they have that existed as of April 30.

Vendors may choose upon written notification to PCI SSC to not list a newly approved device for up to a maximum of six months. However, all approved devices for which the approval has not expired shall be billed an approval-listing fee for all such approvals that existed as of May 1. Vendors shall not be billed the annual listing fee for products for which they have notified PCI in writing that they no longer market for new deployments. This applies only to an entire approval, and not individual items within an approval. The product(s) will continue to be listed by PCI 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. In all cases, vendors will not be allowed to manipulate product listings to avoid the listing or maintenance fee.

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 testing lab may perform a pre-assessment 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.

Test Dates

Vendors submitting devices for testing at a PCI-recognized laboratory will be assigned a test date by the lab. Vendors should notify the laboratory directly of any delay in submitting payment security devices for testing.

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. PCI expects that a best-case scenario for a full evaluation suite will take a minimum of four to six weeks of laboratory work. This assumes one test cycle, but many test cycles may be required. 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.

Test Cycle Definition

All payment security devices are required to complete a test cycle with successful results as part of the PCI Testing and Approval 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 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.

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, a vendor contact should be "on call" to discuss discrepancies and respond to questions from the laboratory.

Approval Process

Release Agreement and Delivery of Report

Prior to the laboratory's releasing the evaluation report, the vendor must sign a consent form, or release agreement to the NDA, giving permission for release of the information to PCI SSC for approval consideration. In addition, the vendor must sign the *PCI PIN Transaction Security Device Security Evaluation Testing Vendor Release Agreement*, which is submitted by the test laboratory along with the report. To be accepted for payment security device approval consideration, the payment security device evaluation reports **must be delivered directly** to PCI SSC by the laboratories.

Vendors or other third parties licensing approved products from other vendors to market or distribute under their own names shall also need to sign a vendor release agreement prior to the issuance of the approval.

In all cases, the vendor release agreement, unless superseded or otherwise terminated in accordance with provisions within the agreement, shall only require a single submission to cover all submitted vendor products.

Roles and Responsibilities

The laboratory's responsibility and authority is 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.

Issuance of Approval

PCI SSC will base their approval solely on the results of the laboratory evaluation report. Upon receipt of the test report for a new evaluation, the PCI SSC have two weeks (14 calendar days) from receipt of that report to identify any technical issues or questions for resolution by the test laboratory. If no issues or questions to the laboratory are identified within this time frame, PCI SSC shall issue an approval letter and post the approval information to the website. 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 issue the approval letter and post the information to the PCI SSC website.

Additional issues or questions that are raised beyond the initial 14-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 test 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 (e.g., an initial 14 calendar days) is the same, and PCI SSC shall issue a revised approval letter and post the revised information to the website unless issues or questions arise in a manner similar to the aforementioned. Delta reports are prepared using the major requirements the payment security device was evaluated against when newly approved.

In all cases, approval letters may be issued sooner if all payment brands positively affirm.

The PCI approval letter and listing on www.pcisecuritystandards.org will contain, at 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

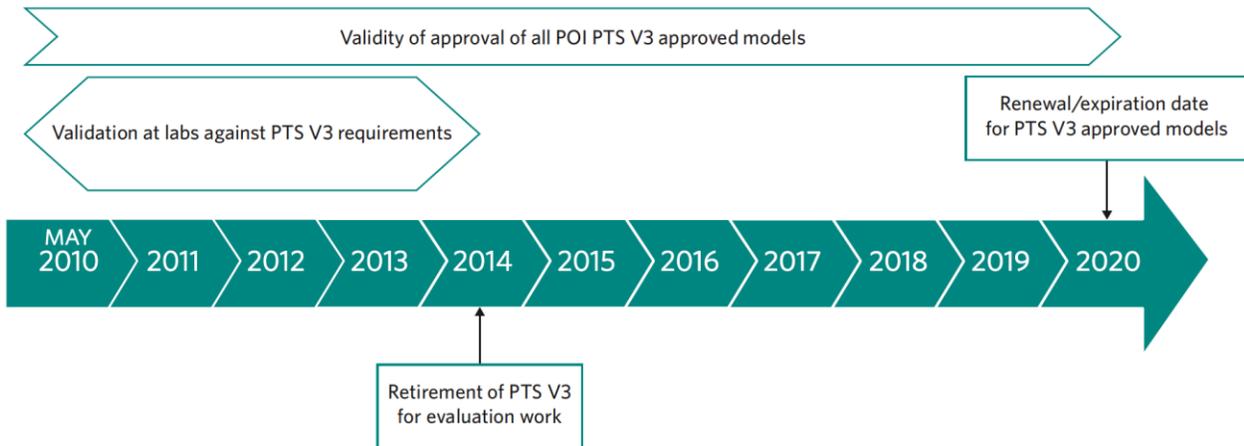
Note:

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

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 PCI PTS standard before the renewal/expiration date, as displayed in the PCI PTS approval list.

The following diagram shows the relationship between the expiration of device model tested under Version 3 of *PCI PTS POI Security Requirements* and its laboratory testing work.



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

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 PCI 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 PCI SSC's website, www.pcisecuritystandards.org.

Note:

If payment security device vendors can modularize the payment security device functionality, it would help minimize re-evaluations due to hardware changes that do not impact payment security device security.

Maintaining Approval

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

If hardware or firmware (including software which 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 as 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 PCI security requirements. PCI SSC will then review the letter to determine whether the change has any impact to the approval status of the payment security device.

Assuming no impact, the new hardware and/or firmware version number would be considered "Approved" and:

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

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

If changes to the device do impact payment security device security requirements, the device must undergo another security evaluation. The laboratory will then submit a new evaluation report to the PCI SSC for re-approval consideration. (In this scenario, the vendor must first submit documentation of the change to the laboratory, which will determine whether the nature of the change impacts payment security device security in accordance with current PCI payment security device security requirements.)

Boundary of Approval

The boundary of approval by which an approval of an existing payment security device model can be carried over to a new (or similar) payment security device model can be accomplished as follows:

1. Vendor describes the design of the new (or similar) payment security device model in the form of a product revision document.
2. Vendor sends the documentation to the selected laboratory for review.
3. Laboratory reviews the documentation (and possibly payment security device samples).
4. Laboratory treats the document review process like a product revision of an existing approved payment security device.
5. Laboratory then sends a letter to the vendor informing it whether or not a full test evaluation will be required.

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.

Notification and Timing

Notwithstanding any other legal obligations the vendor may have, the vendor must immediately notify the PCI Security Standards Council (“Council”) 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 or will have.

Note:

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

Notification Format

The vendor’s initial notification of a security breach or compromise must take the form of a phone call to PCI SSC, followed by an e-mail, fax, or letter providing full details of the security breach or compromise.

Notification Details

Following notification of a security breach or compromise, the vendor must supply the 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 *Payment Card Industry PIN Transaction Security Device Security Evaluation Testing 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.

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 PCI payment brand participants 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 and 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 PCI SSC's *Payment Card Industry PIN Transaction Security Device Security Evaluation Testing Vendor Release Agreement*, using PCI-recognized laboratories to identify the cause of the compromise.

Withdrawal of Approval

PCI SSC reserves the right to withdraw approval of a POI device or HSM and accordingly update the *PCI PTS Device Approval 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 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 does not either meet contractual obligations vis-à-vis PCI SSC or strictly follow the terms of participation on the PCI PTS program as described in this document or the *Payment Card Industry PIN Transaction Security Device Security Evaluation Testing Vendor Release Agreement*.

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 PCI Security Standards Council recognized laboratory. If any aspect of the payment security device is different from that which was tested by the laboratory—even if the payment security device conforms to the basic product description contained in the 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, 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," nor 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. 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 noninfringement, 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 payment brand participants.

Glossary of Terms and Acronyms

Term	Definition
Approval Class	The approval class describes which evaluation requirements the approved device has been tested against. See <i>Appendix A</i> .
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.
Evaluation Framework	Set of requirements for vendors, test methodology for laboratories, approval process for products, and 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 <i>Appendix A</i> .
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
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
PCI PTS Device Security Evaluation Program	The PCI SSC evaluation framework for payment system devices
PED	PIN entry device; approval class aimed at devices with PIN-entry and PIN-processing ability, either attended or unattended, whose primary purpose is to capture and convey the PIN to an ICC reader 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 <i>Appendix A</i> .
POI	Point of interaction
POI Device	Device used in the point of interaction with a consumer
Product Type	The product type describes both the approval class of a device and whether the device is a module to be integrated (OEM) or not.
PTS	PIN Transaction Security, the PCI SSC framework for payment security devices. Refers to POI devices and HSMs, collectively.
PTS Devices	Payment security devices, POI devices, and HSMs
PTS-HSM	The sub-framework of the PCI-PTS device security framework that addresses the security of HSMs
PTS-POI	The sub-framework of the PCI-PTS device security framework that addresses the security of consumer-facing devices

Term	Definition
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 <i>Appendix A</i> .

Appendix A: Device Listing on PCI SSC Website

Listed below are the characteristics of a device listing on the PCI SSC Website.

Point of Interaction (POI)

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

A device that provides for the entry of PINs, 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 online and/or offline PIN entry, and has a clearly defined physical and logical boundary for all functions related to PIN entry.

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

Secure Card Readers must be validated to the Core and SRED 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 Device Management 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 property prefixed with the word “OEM” on the main page of 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 participants’ customers or their agents can be certain of acquiring a POI that has been approved by PCI.

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.

Device Identifier

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

- Model Name,
- Hardware #,
- Firmware #, and
- Application #, if applicable

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 PIN Entry Device Identifier or the Hardware Security Module Identifier.

Table 1: Example of a Device Identifier (four components)

Component	Description
POI Model Name/Number	Acme 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 PCI 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.

Hardware

Hardware # represents the specific hardware component set used in the approved payment security device. The fields that make up the Hardware # may consist of a combination of fixed and variable alphanumeric characters. A lower-case "x" is used by PCI to designate all variable fields. The "x" represents fields in the 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 security requirements or the vendor's approval. To ensure that the payment security device has been approved, acquiring customers or their designated agents are strongly advised to purchase and deploy only those payment security devices with the Hardware # whose fixed alphanumeric characters match exactly the Hardware # depicted on the PCI PTS Device Approval List or the vendor's approval letter from PCI SSC.

Note:

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

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 payment security device security requirements

Table 2: Examples on the Use of Hardware #s

Hardware # of Payment Security Device in the Approval 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 in order for the PTS device to be considered an approved payment security device (hardware component).
NN-4x1-0x0-Ax	Hardware # NN-4x1-0x0-Ax of the Device Identifier does employ the use of 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 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 website lists NN-4x1-0x0-Ax 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 website lists NN-4x1-0x0-Ax 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).

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.

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 may 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 OEM products that are “bolt on” or drop in type modules 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, and in addition, as an approved component of the UPT product, similar to the way other OEM products are listed.

Approval Class

The **Approval Class** is used by PCI 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 PCI PTS Device Security Evaluation Program, regardless of the designated Approval Class, carry PCI’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 PCI PTS Device Security Requirements.

Table 3: Approval Class Descriptions

Approval Class	Description	Specific Features <i>(see Table 4 below for detail)</i>
<p>PED</p>	<p>An approval class aimed at 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.</p> <p>This class may cover both attended and unattended environments and OEM or stand-alone products.</p>	<ul style="list-style-type: none"> ▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology ▪ SRED ▪ OP

Approval Class	Description	Specific Features <i>(see Table 4 below for detail)</i>
EPP	<p>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.</p> <p>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 just 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 in order to obtain overall approval of the UPT.</p>	<ul style="list-style-type: none"> ▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology ▪ SRED ▪ OP
HSM	<p>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:</p> <ul style="list-style-type: none"> ▪ PIN Processing ▪ 3-D Secure ▪ Card Verification ▪ Card Production and Personalization ▪ EFTPOS ▪ ATM Interchange ▪ Cash Card Reloading ▪ Data Integrity ▪ Chip Card Transaction Processing 	N/A

Approval Class	Description	Specific Features <i>(see Table 4 below for detail)</i>
UPT	<p>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:</p> <ol style="list-style-type: none"> 1. Automated Fuel Dispenser 2. Ticketing Machine 3. Vending Machine <p>UPTs may have a compound architecture directly combining payment and the delivery of services and/or goods.</p>	<ul style="list-style-type: none"> ▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology ▪ SRED ▪ OP
SCR	<p>An encrypting card reader that is intended for use with a POI device and may be further defined as an OEM product type to be integrated into a POI terminal.</p>	<ul style="list-style-type: none"> ▪ ICCR ▪ MSR
Non-PED	<p>Non-PIN-acceptance devices validated to the Secure Reading and Exchange of Data Module and, if applicable, the Open Protocols Module. These POI devices are NOT approved for PIN acceptance.</p>	<ul style="list-style-type: none"> ▪ SRED ▪ OP

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.

Expiry Date

The expiration date for PCI-approved devices is the date upon which the device's approval expires.

Requirements Version Used During Evaluation At Laboratory	Expiration of Requirements	Approval Expiration Of Device Models
Version 3.x of <i>PCI PTS POI Security Requirements</i>	April 2014	April 2020
Version 2.x <i>PCI PED or EPP Security Requirements</i>	April 2011	April 2017
Version 1.x of the <i>HSM or UPT Security Requirements</i>	TBD	April 2017
Version 1.x <i>PCI PED or EPP Security Requirements</i>	April 2008	April 2014,

Approvals for PCI-evaluated devices expire six years past the effective date of a subsequent update of the PCI security requirements

Note:

Readers should note that the approval cycle for PCI-approved devices is different than that of pre-PCI approved devices. Approvals for most pre-PCI devices ended on 31 December 2007.

Specific Features per Approval Class

Table 4: Specific Features

Feature and Applicability	Description
<p>PIN Support (PED, EPP, UPT)</p>	<p>“PIN Support” denotes the type of PIN entry verification that can be supported by the POI.</p> <p>“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 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 for that channel. “Offline” means that the POI has the capability to support offline PIN verification by the payment card’s integrated chip.</p> <p>Unless otherwise noted, the “Offline” designation, without any suffix, in the <i>PCI PTS Device Approval List</i> represents that the POI has the capability to support both plain-text 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 plain-text offline PIN verification.</p> <p>However, under current testing, all newly evaluated offline POI devices must support both plain-text and enciphered PIN verification</p>
<p>Key Management (PED, EPP, UPT)</p>	<p>“Key management” denotes whether the laboratory has successfully evaluated the payment security device to support the use of Triple DES (TDES) for PIN encryption for online PIN. TDES requires use of at least a double-length key.</p> <p>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 scheme(s).</p>

Note:
All newly approved offline PIN verification POIs must support both plain-text and enciphered PIN verification.

Note:
DUKPT is the only “unique key per transaction” (UKPT) algorithm (ANSI X9.24) that PCI recognizes and approves; all other forms of UKPT tested by the laboratory will not be depicted in the approval letter or on the PCI PTS website.

Feature and Applicability	Description
<p>Prompt Control (PED, EPP, UPT)</p>	<ul style="list-style-type: none"> ▪ Vendor-controlled: The end-user, acquirer, or reseller cannot modify the attended POS 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 attended POS 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. <p>Not applicable for devices without a display.</p> <p>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.</p>
<p>PIN-Entry Technology (PED, EPP, UPT)</p>	<p>“PIN-entry technology” denotes which technology is implemented in order to capture the cardholder PIN. The value for this field can be:</p> <ul style="list-style-type: none"> ▪ 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.
<p>Approved Components (PED, UPT)</p>	<p>“Approved components” contains, when relevant, the list of approved subcomponents that are part of the approved device, and which have successfully undergone a distinct evaluation.</p> <p>Each component is listed with its approval number. Moreover, if the component belongs to the EPP approval class, the approval number is augmented with the “EPP” qualifier.</p>
<p>Functions Provided (PED, EPP, UPT, SCR, Non-PED)</p>	<p>“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:</p> <ul style="list-style-type: none"> ▪ PIN entry: The device enables cardholder PIN capture. ▪ Card reader capabilities: The device has components that can capture card data, such as magnetic-stripe reader (MSR) or ICC reader (ICCR). ▪ Display: The device has an integrated display used for cardholder prompts. ▪ SRED: The device has met the requirements in the Secure Reading and Exchange of Data module ▪ OP: The device has met the requirements in the Open Protocols module
<p>Device Form Factor</p>	<p>All security relevant components (PIN pad, display, card reader(s)) of the device are shown in one or more pictures.</p>