Payment Card Industry (PCI)

PIN Transaction Security (PTS)

Device Testing and Approval Program Guide

Version 1.1

August 2009

Document Changes

Date	Version	Description
April 2009		▪ Add HSM and UPT requirements ▪ Changed terminology to reflect new framework naming
August 2009	1.1	Final edits

Table of Contents

Related Publications

The PTS Security framework consists of the following manuals that contain the physical and logical security requirements for all payment security devices, as well as device management requirements for activity prior to initial key loading. The manuals listed below are specific to the particular payment security device approval class being evaluated, i.e., POS PED, HSM, UPT or EPP.

- *Payment Card Industry (PCI) POS PIN Entry Device Security Requirements*
- *Payment Card Industry (PCI) Encrypting PIN PAD (EPP) Security Requirements*
- *Payment Card Industry (PCI) Unattended Payment Terminal (UPT) Security Requirements*
- *Payment Card Industry (PCI) Hardware Security Module (HSM) Security Requirements*
- *Payment Card Industry (PCI) PIN Transaction Security Device Security Evaluation Testing Vendor Release Agreement*

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.

The following additional documents are used in conjunction with the aforementioned:

- *Payment Card Industry (PCI) POS PIN Entry Device Evaluation Vendor Questionnaire*
- *Payment Card Industry (PCI) Encrypting PIN Pad (EPP) Evaluation Vendor Questionnaire*
- *Payment Card Industry (PCI) Unattended Payment Terminal (UPT) Evaluation Vendor Questionnaire*
- *Payment Card Industry (PCI) Hardware Security Module (HSM) Evaluation Vendor Questionnaire*
- *Payment Card Industry (PCI) POS PIN Entry Device Derived Test Requirements*
- *Payment Card Industry (PCI) Encrypting PIN Pad (EPP) Derived Test Requirements*
- *Payment Card Industry (PCI) Unattended Payment Terminal (UPT) Derived Test Requirements*
- *Payment Card Industry (PCI) Hardware Security Module (HSM) Derived Test Requirements*

The four Security Requirements manuals list the specific technical requirements and provide the forms used to measure compliance. The four Vendor Questionnaires solicit additional information from vendors to support their claims of the conformity of their devices to those requirements. The Derived Test Requirements (DTRs) provide specific direction to vendors on methods the test laboratories may apply when testing against the requirements.

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 PIN entry devices and hardware security modules, collectively referred to as “payment security devices.” As such, PCI SSC has agreed that, in general, all relevant security requirements and associated test requirements will be updated every three years. To make the introduction of new requirements easier for vendors, PCI SSC has agreed to release updated requirements documents one year in advance of the actual implementation. For example, requirements defined in a document released on 30 April 2007 became effective from 30 April 2008.

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 customers[1] and vendors to help reduce the impact of any changes.

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 for 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 (POIs)" devices refers broadly to all PIN-acceptance devices, and both attended and unattended point-of-sale (POS) devices, as well as encrypting PIN pads used in consumer-facing transactions. Other consumer-facing device types 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 POIs 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.

[1] Customers are financial institutions that:

a) Offer payment cards (issuers) for one or more of the participating payment brands;

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 PTS Devices.

About the PCI Security Standards Council

Under the auspices of the Payment Card Industry (PCI) Security Standards Council, the American Express, Discover, JCB, MasterCard, and Visa payment organizations have established the PIN Transaction Security Group with responsibility for the standardized security requirements, testing methodologies, and procedures for payment security devices. All devices submitted for security evaluations and approved have been evaluated against the applicable aligned Payment Card Industry (PCI) PTS Security Requirements. The PCI Approval Lists provide a full list of products recognized as meeting PCI 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 sensitive data, such as cardholder-entered PINs, 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.

PTS Security Alignment Initiative and Requirements

The Payment Card Industry (PCI) has initiated a collaborative effort to address common industry security criteria, including the security-related aspects of payment security devices. The PCI alignment related to payment security devices represents an effort to standardize device security requirements relevant to the protection of sensitive data (such as PIN and cryptographic-key protection), the device-testing methodologies utilized, and the approval processes employed.

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 process.

Payment Brand Rules

In addition to coordinating security requirements with its PCI partners, it is the responsibility of the individual payment brand to generate and issue mandates relating to the adherence of vendors, acquirers and merchants to the PCI PTS programs.

Testing and Approval Process Description

Overview

With the new PCI alignment, vendors may contact one of the PCI-recognized laboratories and complete the appropriate PCI forms *(PCI Security Requirements* and *PCI Vendor Questionnaire).* The vendor will then submit the device, together with any additional documentation required by the laboratory, for evaluation against the PCI Security Requirements. Upon completion of the evaluation, PCI SSC will review the evaluation report to check for compliance. When the product meets the PCI requirements, an approval letter will be issued, confirming successful completion of the process. Once the device is approved, the product will be listed on the PCI PTS website.

Prior to Testing (POI only)

- PCI SSC recommends that the POI receive EMV Level 1 approval first, if applicable, and then POI 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 POI security approval.)
- If the POI 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. If you want the POI's approval to indicate support of both options, after the second PIN-entry option evaluation has been performed ensure that the laboratory includes both in its report.

Testing Process

Payment security devices are evaluated using the requirements embodied in the PCI Security Requirements for POS PED, EPP, or UPT, as appropriate (collectively, "POI manuals"), or *PCI Hardware Security Module Requirements* manual ("HSM manual") as applicable, specifically the Physical and Logical Security sections. 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. The laboratory does not evaluate the payment security devices to the Device Management Requirements as specified in the *PCI POI 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.

Unlike the EMVCo-recognized laboratories used for EMV testing, which perform offline PIN functionality testing only, the PCI-recognized payment security device laboratories focus on online and offline PIN security testing for POIs.

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

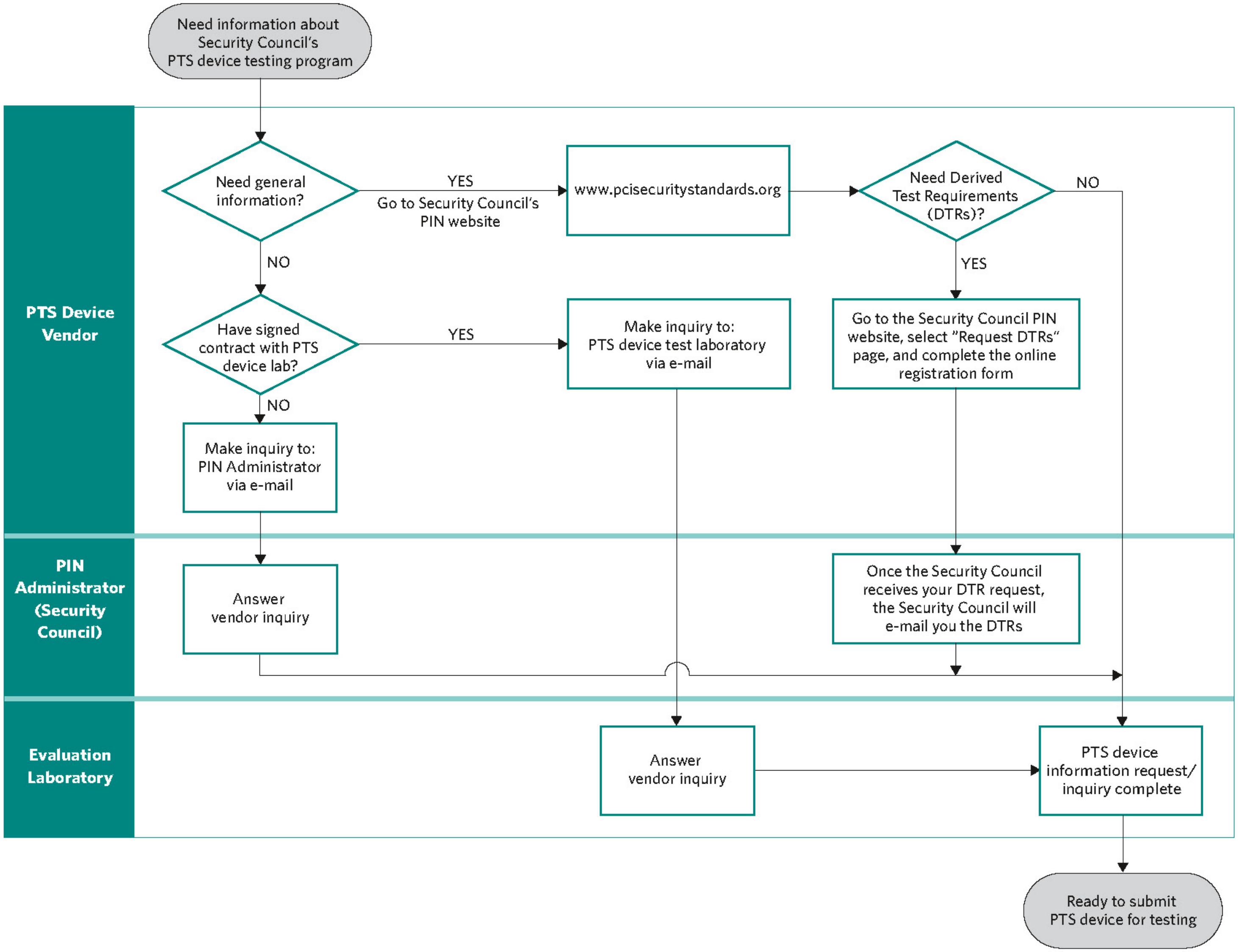

Need information about Security Council's PTS device testing program
PTS Device Vendor
PIN Administrator (Security Council)
Evaluation Laboratory
Need general information?
YES
Go to Security Council's PIN website
www.pcisecuritystandards.org
Need Derived Test Requirements (DTRs)?
NO
YES
NO
Have signed contract with PTS device lab?
YES
Make inquiry to: PTS device test laboratory via e-mail
Go to the Security Council PIN website, select "Request DTRs" page, and complete the online registration form
NO
Make inquiry to: PIN Administrator via e-mail
Answer vendor inquiry
Once the Security Council receives your DTR request, the Security Council will e-mail you the DTRs
Answer vendor inquiry
PTS device information request/ inquiry complete
Ready to submit PTS device for testing

Figure 2: PTS Device Approval Flow Chart

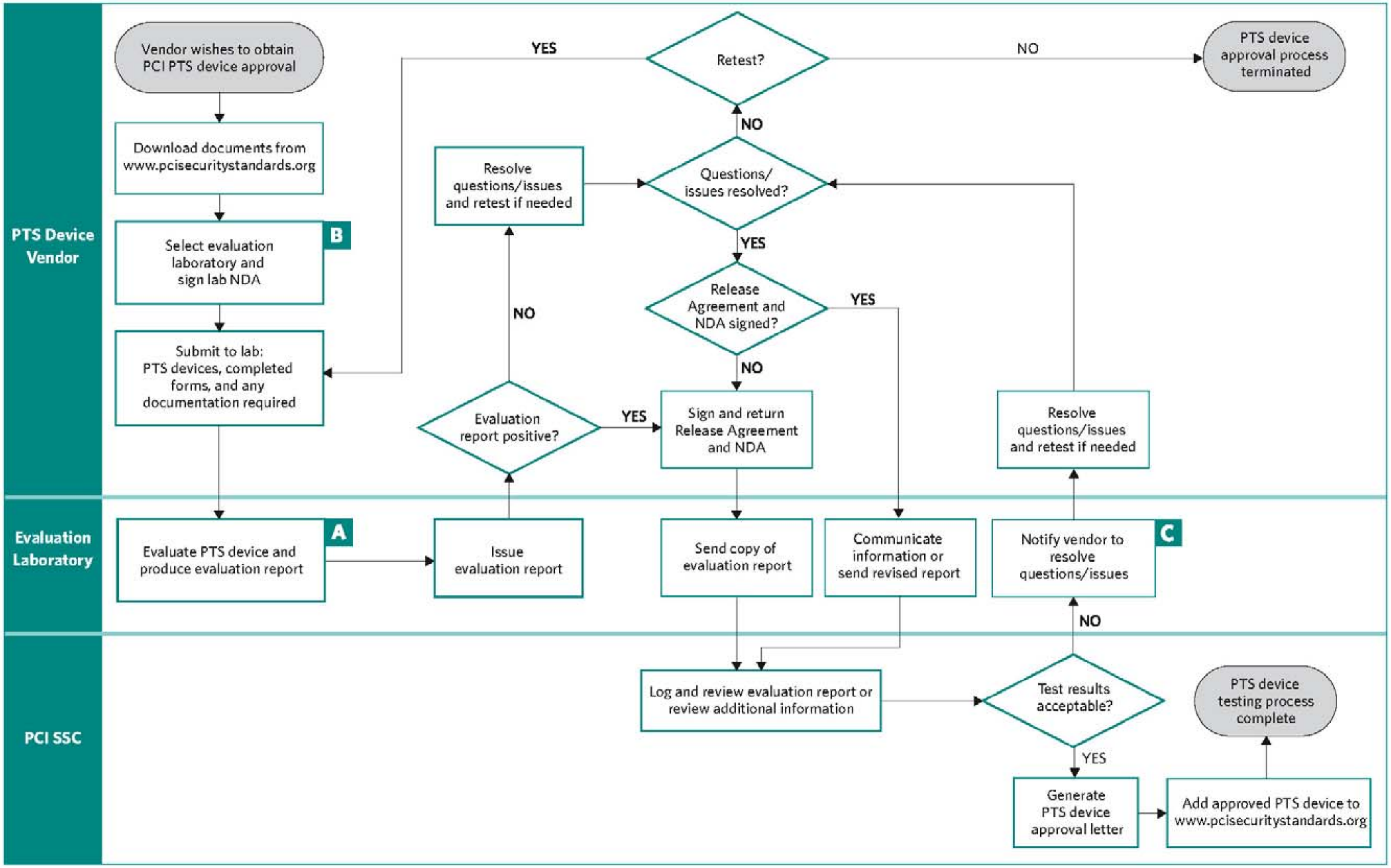
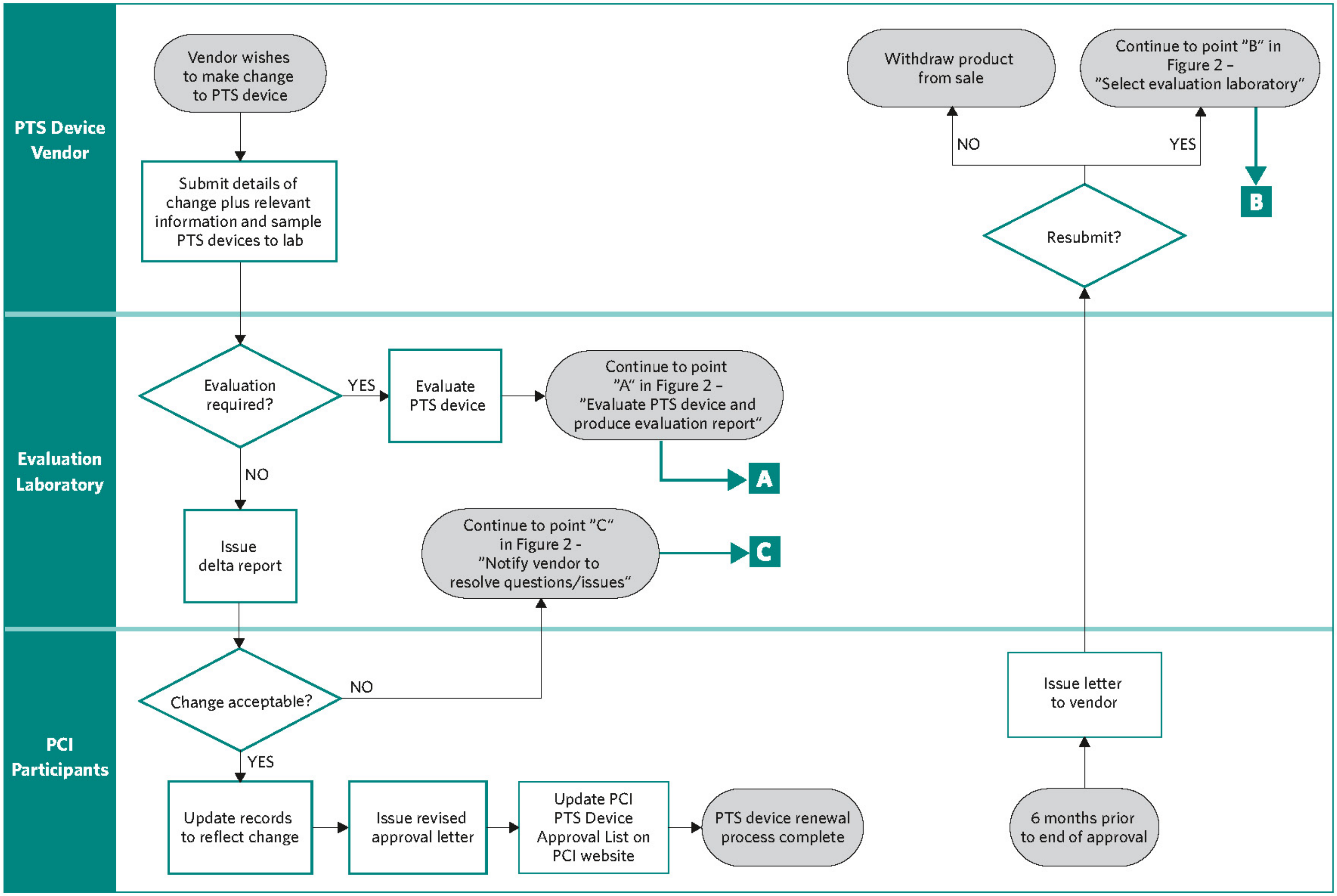

PTS Device Vendor
Evaluation Laboratory
PCI SSC
Vendor wishes to obtain PCI PTS device approval
Download documents from www.pcisecuritystandards.org
Select evaluation laboratory and sign lab NDA
B
Submit to lab: PTS devices, completed forms, and any documentation required
Evaluate PTS device and produce evaluation report
A
Issue evaluation report
Evaluation report positive?
NO
YES
Resolve questions/issues and retest if needed
Retest?
YES
NO
PTS device approval process terminated
NO
Questions/ issues resolved?
YES
Release Agreement and NDA signed?
YES
NO
Sign and return Release Agreement and NDA
Send copy of evaluation report
Communicate information or send revised report
Resolve questions/issues and retest if needed
Notify vendor to resolve questions/issues
C
NO
Log and review evaluation report or review additional information
Test results acceptable?
YES
Generate PTS device approval letter
Add approved PTS device to www.pcisecuritystandards.org
PTS device testing process complete

Figure 3: PTS Device Change Request and Renewal Flow Chart


PTS Device Vendor
Evaluation Laboratory
PCI Participants
Vendor wishes to make change to PTS device
Submit details of change plus relevant information and sample PTS devices to lab
Withdraw product from sale
Continue to point "B" in Figure 2 – "Select evaluation laboratory"
NO
YES
B
Resubmit?
Evaluation required?
YES
Evaluate PTS device
Continue to point "A" in Figure 2 – "Evaluate PTS device and produce evaluation report"
A
NO
Issue delta report
Continue to point "C" in Figure 2 - "Notify vendor to resolve questions/issues"
C
Change acceptable?
NO
YES
Issue letter to vendor
Update records to reflect change
Issue revised approval letter
Update PCI PTS Device Approval List on PCI website
PTS device renewal process complete
6 months prior to end of approval

Detailed Evaluation Process

Payment security devices will be evaluated against the PCI Security Requirements for POS PED, EPP, or UPT, as appropriate (collectively, "POI manuals"), or the *Payment Card Industry Hardware Security Module Security Requirements* manual, specifically the Physical and Logical Security core sections. 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.

Though the information is required by PCI, the laboratory does not evaluate the payment security device for the Device Management Requirements as specified in the above-mentioned manuals. 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.

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 POIs (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 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 that terminal was ever compromised in the field, the retained samples may be used to investigate any compromise or security breach. Devices should be sent to:

Attn: Jeremy King
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 or HSM.

PCI-Recognized Laboratories

PCI SSC currently recognizes the following laboratories for PTS device testing. PCI may recognize more labs in the future based on defined business needs.

Laboratory	Contact Information	Address
Brightsight	Mr. Rob van Marrewijk marrewijk@brightsight.com, pci@brightsight.com Phone: +31 15 269 2522 Fax: +31 15 269 2555	Delftechpark 1 2628 XJ Delft, The Netherlands www.brightsight.com
DOMUS IT Security Laboratory	Mr. Marc Boire or Mr. Jason Lawlor info@domusitsl.com Phone: 1 613 726-5019 Fax: 1 613 248-4948	400 March Road, Suite 190 Ottawa, Ontario K2K 3H4 Canada www.domusitsl.com
EWA-Canada Ltd	Mr. Paul Zatychec or Mr. Steven Bowles pcilab@ewa-canada.com Phone: +1.613.230.6067, x1227 Fax: +1.613.230.4933	55 Metcalfe Street, Suite 1600 Ottawa, Ontario K1P 6L5 Canada www.ewa-canada.com
InfoGard Laboratories, Inc.	Mr. Steve Wilson or Mr. Adam Hardcastle ped@infogard.com Phone: +1.805.783.0810 Fax: +1.805.783.0889	709 Fiero Lane, Suite 25 San Luis Obispo, California 93401 U.S.A. www.infogard.com
RFI Global Services Ltd	Mr. Barry Gilbert enquiries@rfi-smart.com Phone: +44 (0) 1256 312081 Fax: +44 (0) 1256 312001	Pavillion A Ashwood Park Ashwood Way Basingstoke, RG23 8BG United Kingdom www.rfi-global.com
SRC Security Research & Consulting GmbH	Mr. Detlef Kraus detlef.kraus@src-gmbh.de Phone: +49 228 2806 101 Fax: +49 228 2806 199	Graurheindorfer Str. 149a D-53117 Bonn Germany www.src-gmbh.de
T-Systems	Mr. Robert Hammelrath robert.hammelrath@t-systems.com Phone: +49 228 9841 114 Fax: +49 228 9841 60	Rabinstrasse 8 53111 Bonn, Germany www.t-systems.com/ict-security
Witham Laboratories	Andrew Jamieson andrew.jamieson@withamlabs.com David McGregor david.mcgregor@withamlabs.com Phone: +61 3 9846 2751 Fax: +61 3 9857 0350	Ground Floor 842 High Street Kew East 3102 Melbourne, Victoria Australia www.withamlabs.com

Fees

Note:

The vendor pays all laboratory evaluation fees directly to the laboratory.

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.

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.

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 beginning with March 31, 2008, 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., 1.x, 2.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., 1.x—to an approval under another major version number, e.g., 2.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, attended POS PEDs and EPPs approved under Version 1 of the respective requirements shall expire with April 30, 2014; Version 2 attended POS PEDs and EPPs shall expire April 30, 2017, and so forth. I.e., on May 1 vendors shall be billed $1,000 per PCI approval for each approval they have that existed as of April 30. Vendors shall not be billed an approval-listing fee for devices that are approved but for which they choose to not have the product listed on PCI SSC website. However, vendors will not be allowed to manipulate product listings to avoid the fee—i.e., vendors cannot have a product pulled from the listing and then request that it be re-listed after the billing.

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.

POI Privacy Shield Requirement

PIN entry must be performed in such a way that cashiers, checkout attendants, and other people nearby cannot easily observe the PIN during entry by the cardholder. Therefore, PCI requires that the Point of interaction be equipped with proper shielding protection for privacy—"to provide a means to deter the visual observation of the PIN values as they are being entered by the cardholder," as specified in the *PCI POI Security Requirements* manual.

In addition to the physical PIN pad design, PCI SSC continues to stress the need for proper PIN pad placement, and for cardholder and customer education, merchant and cashier training, and policy enforcement. PCI's POI privacy shield requirements differentiate between POIs that are considered to be handheld devices and POIs that are used in attended and unattended environments.

Note:

The privacy shield requirements facilitate deterring PIN entry observation within the installed POI's surrounding environment, although some specific national markets may not permit this consideration.

Attended environments include POS devices used in merchant locations, and unattended include ATMs/Cash Dispensers, POS kiosks, and self-service gas pumps. Meeting PCI's privacy shield requirements may include, but is not limited to, use of:

- A physical shielding barrier,
- Limited viewing angle (for example, a polarizing filter or recessed PIN pad),
- Housing that is part of the ATM or kiosk, cardholder's hand or body (applies to handheld POIs only), and
- The installed POI's environment.

The PCI-recognized test laboratories will determine whether the POI has properly met the PCI privacy shield requirements.

Practical experience has shown that privacy shields are sometimes removed, not used, or not purchased. The rationale may be that they are deemed bulky or obtrusive, make it more difficult to see the POI's screen, or, with less dexterous users, interfere with card payment and PIN entry. Although cardholders may prefer to use their hands or bodies to shield PIN entry, PCI SSC requires that the POI meet the privacy shield requirements, as evaluated by the laboratory, in order for the POI to be approved by PCI.

PCI SSC continues to assist POI vendors, as well as the industry in general, with understanding the PCI policy on privacy shields. Acquirers should ensure, where possible, that they are able to take action against any merchants who breach this privacy shield policy through their merchant contracts.

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 PCI SSC's *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, "Payment Security Device Characteristics."

- 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

PTS Device Approval Renewal Process

Approximately six months before the payment security device's approval is due to expire, PCI SSC will notify the vendor regarding whether the vendor intends to renew the approval. The two options available for vendor consideration are:

1. Allowing PCI SSC to remove the payment security device from the Approval List after the expiry date, or
2. Contacting a PCI-recognized laboratory and submitting the appropriate documentation.

With the second option, the laboratory will determine whether the payment security device needs to undergo a full re-evaluation against the current PCI payment security device security requirements, and notify the vendor accordingly.

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 the PCI PTS Coordinator, 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 PTS Coordinator 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 products, as listed in the *PCI PTS Device Approval List*, PCI SSC will take the following actions:

- Notify PCI SSC 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 or HSM and remove that payment security device from the *PCI PTS Device Approval List*, when 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.

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 *Appendix A.*
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 *Appendix A.*
OEM	Original equipment manufacturer
Payment Security Device	Any device (for example, a 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 *Appendix A.*
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
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

Term	Definition
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 PCI SSC Website.

Point of Interaction (POI)

For purposes of these requirements, a **POI** 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.*

A POI 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 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.

POIs 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.

POIs 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 #	ver. 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 anytime to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device color, etc.

Note:

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

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:

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-4**x**1-0**x**0-A**x**	Hardware # NN-4**x**1-0**x**0-A**x** 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-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 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).

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 a 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.

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** *(see Table 4 below for detail)*
PED	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. This class may cover both attended and unattended environments and OEM or stand-alone	▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology

Approval Class	Description	Specific Features *(see Table 4 below for detail)*
	products.	
EPP	An approval class aimed at secure PIN entry and encryption modules in an unattended PIN-acceptance device, which has met the security requirements detailed in the *Payment Card Industry Encrypting PIN Pad Security Requirements* manual. 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 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.	▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology
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	N/A

Approval Class	Description	Specific Features *(see Table 4 below for detail)*
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 ▪ Prompt control ▪ Key management ▪ PIN-entry technology

Version

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

Expiry Date

The renewal/expiration date for PCI-approved devices is the date by which a vendor must get the device re-evaluated against the current security requirements in order to maintain the approval.

- The renewal/expiration date for pre-PCI approved POS devices is fixed at 31 December 2007.
- The renewal/expiration date for pre-PCI approved EPP devices is the latter of 31 December 2007 or the natural expiration of the original three-year approval (as late as September 2008).
- Approval for devices tested using Version 1.x PCI PED or EPP Security Requirements expire April 2014, six years from the 2008 effective date of Version 2.
- Approval for devices tested using Version 2.x PCI PED or EPP Security Requirements expire April 2017, six years from the 2011 effective date of Version 3.
- Approval for devices tested using Version 1.x of the HSM or UPT Security Requirements expire April 2017, six years from the 2011 effective date of Version 2.

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 to expire date among all evaluations, including the embedded device itself.

Pre-PCI approved devices are not under PCI SSC's purview and cannot have their approvals extended unless they are submitted for approval against the current PCI requirements to receive a new renewal/expiration date from PCI SSC.

Approvals for PCI-evaluated devices expire six years past the effective date of a subsequent update of the PCI security requirements. The objective is a six-year minimum approval life expectancy, barring a severe threat that may require immediate changes. In order for entities required by individual participating payment brands to retain protection from liability due to compromise of the devices, these entities may only purchase devices on the current approved list. Nevertheless, they can continue to deploy existing inventory that was purchased and delivered prior to the device's scheduled approval expiration.

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.

There is currently no sunset date for devices that were on the approved list at the time of deployment. Deployed devices that have their approvals expire may continue to be used. The expiration timeframe is associated with new purchases/deployments, not existing deployments. The PCI payment brand participants expect that in the future, the PCI participants will determine a sunset date for pre-PCI approved devices.

Specific Features per Approval Class

Table 4: Specific Features

Feature and Applicability	Description
PIN Support (PED, EPP, 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 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. Unless otherwise noted, the "Offline" designation, without any suffix, in the *PCI PTS Device Approval List* 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. However, under current testing, all newly evaluated offline POI devices must support both plain-text and enciphered PIN verification ***Note:*** *All newly approved offline PIN verification POIs must support both plain-text and enciphered PIN verification.*

Feature and Applicability	Description
Key Management (PED, EPP, UPT)	**“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. 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). ***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.*
Prompt Control (PED, EPP, UPT)	▪ **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. 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 (PED, EPP, 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.
Approved Components (PED, UPT)	**“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. 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.

Feature and Applicability	Description
Functions Provided (EPP, OEM PED)	"**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: ▪ **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.