Payment Card Industry (PCI)

PIN Transaction Security (PTS)

Device Testing and Approval Program Guide

Version 1.6

October 2016

Document Changes

Date	Version	Description
September 2010	1.0	Initial Release
October 2011	1.1	Add approval classes for encrypting card readers and non-PEDs
July 2012	1.2	Added HSM v2 and clarifications for Fees, Approval Classes, and Expiry Dates
September 2013	1.3	Updated for POI v4 and clarification for Integration, Open Protocols, SRED, device archival, determination of approval status, delta evaluations, submittal deadlines, fees, secure card readers and non-PEDs
March 2014	1.4	Changes in device sample requirements. Additions to compromise notification process. Defined new device category—*Devices with Expired Approval*. Provided additional clarifications for Approval Class Features—PIN support, Key management, and Functions Provided. Updated definitions for non-PEDs and SCRs. Further explanations on the delta-evaluation process.
2015	1.5	Modified process for requesting change of business name/address/contact details via an Administrative Change Request Form submitted to the lab; change to invoice cycle; pro-rated invoices issued November 1 for all devices listed between May 2 – October 31. New guidance on licensing (re-branding) of another vendor's device.
2016	1.6	Updated for POI v5 and HSM v3. Testing timeframes restated. Added new HSM approval class information for Key Loading Devices and Remote Administration Platforms. Clarifications to product types for self-contained OEM products.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Table of Contents

Document Changes ..... **i**
1 Introduction **1**
1.1 Related Publications 1
1.2 Updates to Documents and Security Requirements 3
1.3 About This Document 4
1.4 About the PCI Security Standards Council 5
1.5 Payment Brand Rules 5
2 Testing and Approval Process Description **6**
2.1 Overview 6
2.2 Prior to Testing (POI devices only) 6
2.3 The Modular approach 7
Table 1: Evaluation Modules *7*
2.4 Testing Process 8
Table 2: Testing and Approval Process Illustration *8*
2.5 Figure 1: PTS Device Testing Inquiry Flow Chart 9
2.6 Figure 2: PTS Device Approval Flow Chart 10
2.7 Figure 3: PTS Device Change Request and Renewal Flow Chart 11
3 Detailed Evaluation Process **12**
3.1 Required Documentation and Materials 13
4 Preparation for Testing **15**
4.1 Laboratory Services 15
4.2 PCI-Recognized Laboratories 15
4.3 Test Fees 15
4.4 Requirements for Testing 15
4.5 Test Dates 15
4.6 Testing Timeframes 16
4.7 Test Cycle Definition 16
4.8 Technical Support throughout Testing 16
5 PCI Fees **17**
5.1 Delinquencies 17
5.2 New Evaluations 17
5.3 Initial Evaluations under Major Versions 17
5.4 Approval-Listing Fee 17
6 Approval Process **18**
6.1 Release Agreement and Delivery of Report 18
6.2 Roles and Responsibilities 18
6.3 Issuance of Approval 18
6.4 Listing Delay 19
6.5 Expiry of Approval 19
7 Changes to a Previously Approved PTS Device **21**
7.1 Maintaining Approval 21
7.2 Boundary of Approval 22
7.3 Rebranding/Licensing 22
7.4 Approval Withdrawal 22
7.5 Administrative Changes 22

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

8 Notification Following a Security Breach or Compromise 23
8.1 Notification and Timing 23
8.2 Notification Format 23
8.3 Notification Details 23
8.4 Actions following a Security Breach or Compromise 24
8.5 Withdrawal of Approval 24
9 Legal Terms and Conditions 25
10 Glossary of Terms and Acronyms 26
Appendix A: Device Listing on PCI SSC Website 28
A.1 Point of Interaction (POI) 28
A.2 Hardware Security Module (HSM) 29
A.3 Devices with Expired Approval 29
A.4 Device Identifier 30
Table 3: Example of a Device Identifier (five components) 30
A.5 Model Name/Number 30
A.6 Hardware # 31
Table 4: Examples on the Use of Hardware #s 31
A.7 Security Policy 32
A.8 Approval Number 32
A.9 Product Type 32
A.10 Approval Class 33
Table 5: Approval Class Descriptions 33
A.11 Version 36
A.12 Expiry Date 36
Table 6: Approval Expiry Dates 36
A.13 Specific Features per Approval Class 38
Table 7: Specific Features 38
Appendix B: Delta Evaluations – Scoping Guidance 41
B.1 Introduction 41
B.2 What is a Delta Evaluation? 41
B.3 Determining Whether a Delta is Permissible 41
B.3.1 Sample Impacts of Certain Changes 42
B.3.2 Firmware Changes 42
Table 8: Firmware Change Types and Impacted Requirements 42
B.3.3 Hardware Changes 43
Table 9: Acceptable Hardware Changes 44
B.4 Engaging a PTS Lab to Perform a Delta Assessment 45
B.5 Delta Documentation Requirements 45
B.5.1 Reporting Guidance for PTS Vendors 45
B.5.2 Reporting Requirements for PTS Laboratories 45
B.6 Applicability of FAQs During Delta Assessments 46
B.7 Considerations for Updated Components in Integrated Terminals 46
Appendix C: PTS Administrative Change Request 47
Supporting Documentation Required 48

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

1 Introduction

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

1.1 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	
▪ *PIN Transaction Security (PTS) Point of Interaction (POI) Modular Security Requirements, v5.0* ▪ *PIN Security Requirements, v2.0* ▪ *PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements, v3.0.0*	Contain the physical and logical security requirements as well as device management requirements for activity prior to initial key loading. Provide the forms to be used by laboratories and vendors.
FAQs	
▪ *PTS POI: Frequently Asked Questions*	General frequently asked questions
▪ *PTS POI Security Requirements Technical FAQs for use with Version 5* ▪ *PTS PIN Security Requirements Technical FAQs for use with Version 2* ▪ *Hardware Security Module (HSM) Technical FAQs for use with Version 3*	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.
Evaluation Vendor Questionnaires	
▪ *PIN Transaction Security (PTS) Point of Interaction (POI) Modular Evaluation Vendor Questionnaire, v5.0* ▪ *PIN Transaction Security (PTS) Hardware Security Module (HSM) Evaluation Vendor Questionnaire, v3.0*	Solicit additional information from vendors to support their claims of the conformity of their devices to those requirements.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

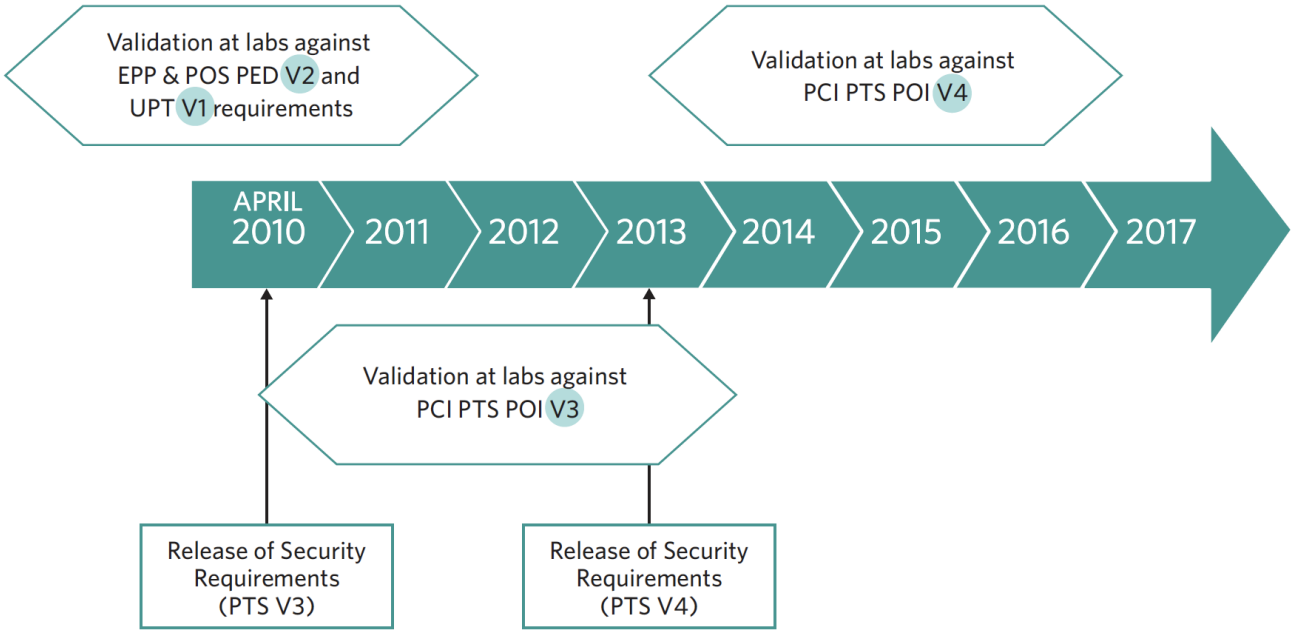
Document Name	Description
Derived Test Requirements	
▪ *PIN Transaction Security (PTS) Point of Interaction (POI) Derived Test Requirements, v5.0* ▪ *PIN Transaction Security (PTS) Hardware Security Module (HSM) Derived Test Requirements, v3.0*	Provide specific direction to vendors on methods the test laboratories may apply when testing against the requirements
Recognized Laboratories List	
▪ *Payment Card Industry (PCI) Recognized Laboratories*	Currently recognized laboratories for PTS device testing.
Vendor Release Agreement	
▪ *Payment Card Industry Vendor Release Agreement*	Contains the terms and conditions that govern the exchange of information between vendors and the PCI SSC
Approved Terminal Models List	
▪ *Approved PIN Transaction Security Devices*	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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

1.2 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 customers[1] 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

1.3 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

1.4 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.

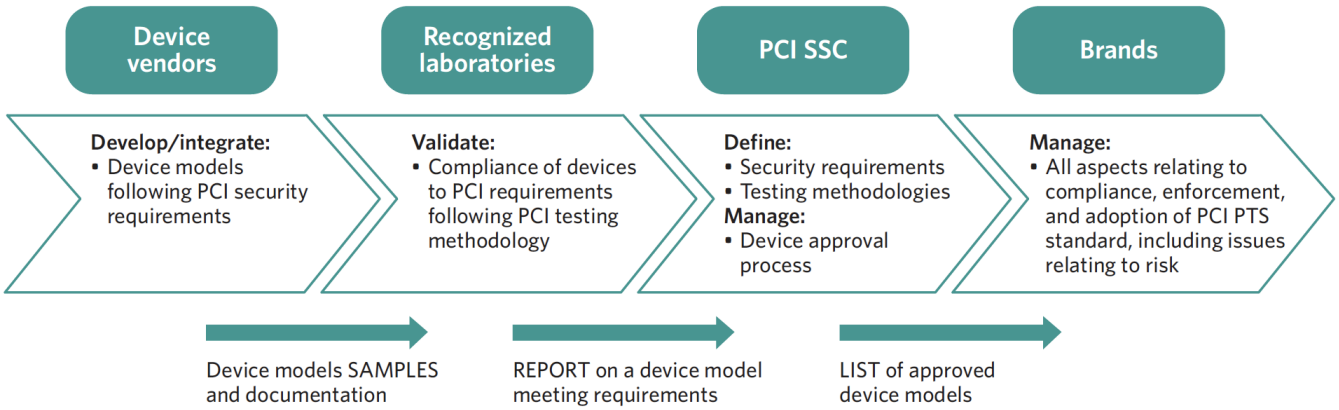
All devices submitted for security evaluations and approval have been evaluated against the applicable aligned Payment Card Industry (PCI) PTS Security Requirements. The PCI Approval Lists provide a full list of payment security devices recognized as meeting PCI PTS Requirements.

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.

1.5 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.

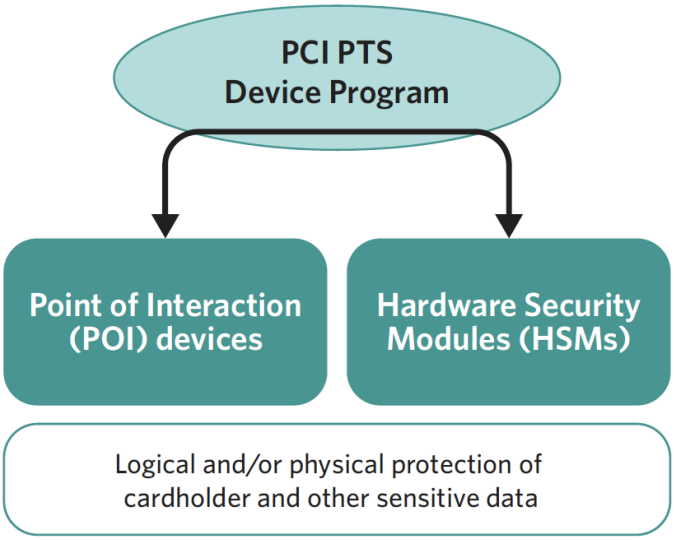


Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2 Testing and Approval Process Description

2.1 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, it will be approved and listed on the PCI PTS website. An approval letter will be issued confirming successful completion of the process.

2.2 Prior to Testing (POI devices only)

- PCI SSC recommends that the POI device receive EMV Level 1 approval first, if applicable, and then PCI 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2.3 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.

Table 1: Evaluation Modules

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 Requirements7	Ensures that the integration of previously approved components does not impair the overall security as stated in the security requirements and includes security management requirements applicable to the integrated device.
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.

Any product that incorporates separate modules—such as an EPP, card readers, etc.—must complete the integration requirements.

Products are not required to support open protocols or the secure reading and exchange of data (SRED); however, if they do, those modules are mandatory for evaluation and approval.

The overall intent of the SRED validation requirement is to ensure that implementations of account data protection are fully robust as evidenced by validation and approval against the SRED module. However, the requirement is not intended to inhibit the vendor from implementing account data protections that are not sufficient to meet the SRED module but which still may provide some lesser level of protection for account data. Thus a vendor implementing account data protections and ***not*** seeking SRED as an approved function provided may do so.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2.4 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.

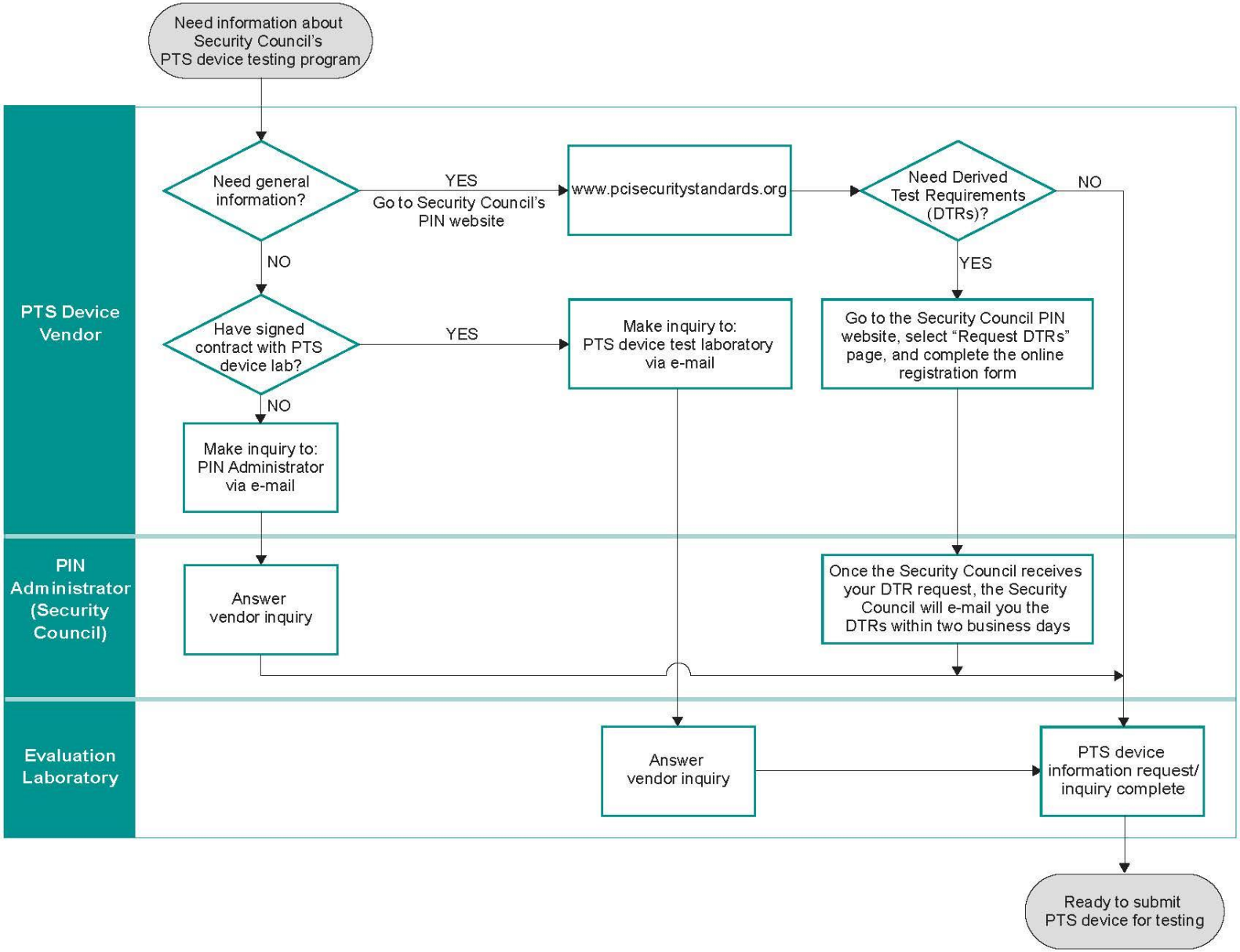
Table 2: Testing and Approval Process Illustration

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

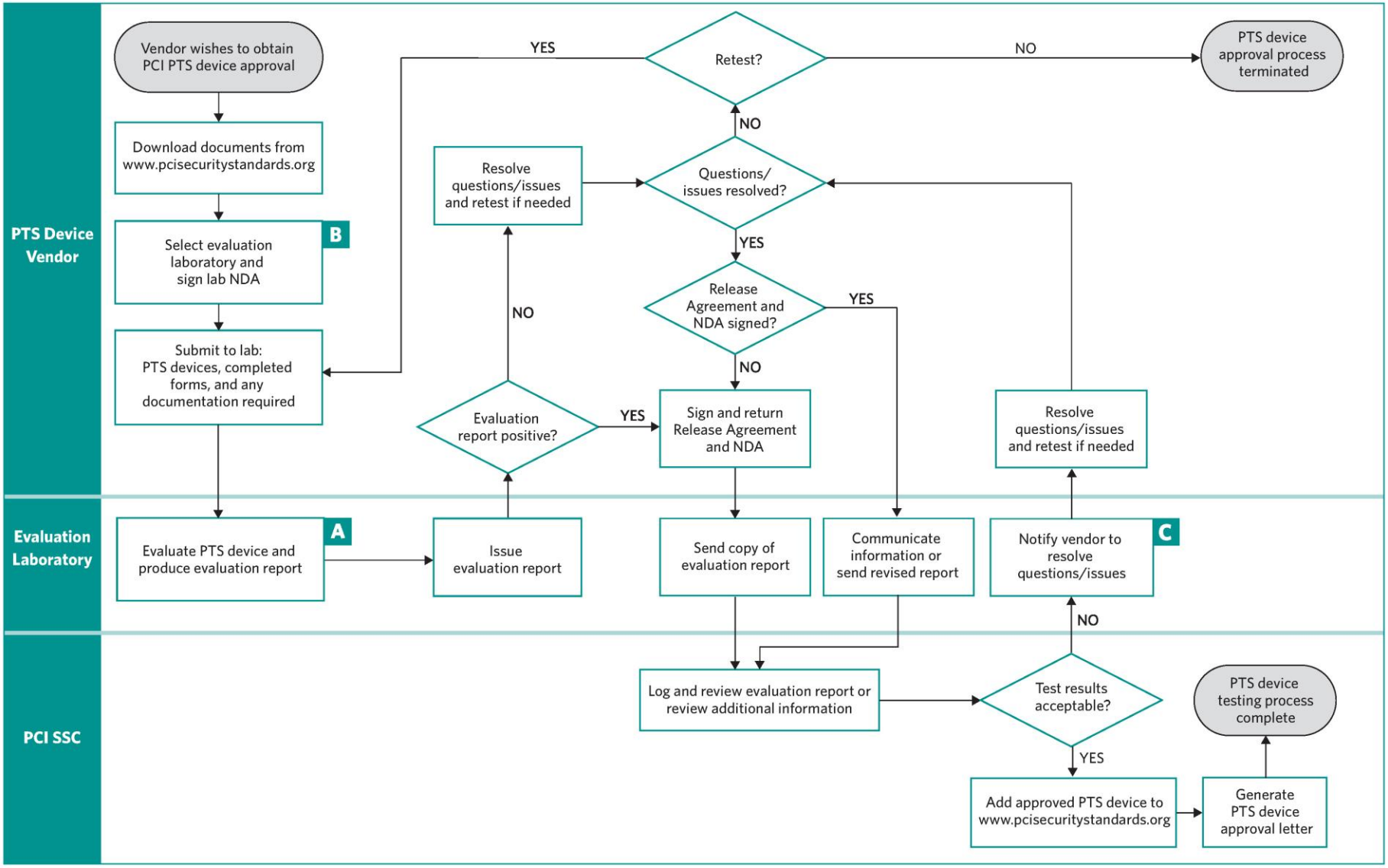
Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2.5 Figure 1: PTS Device Testing Inquiry Flow Chart



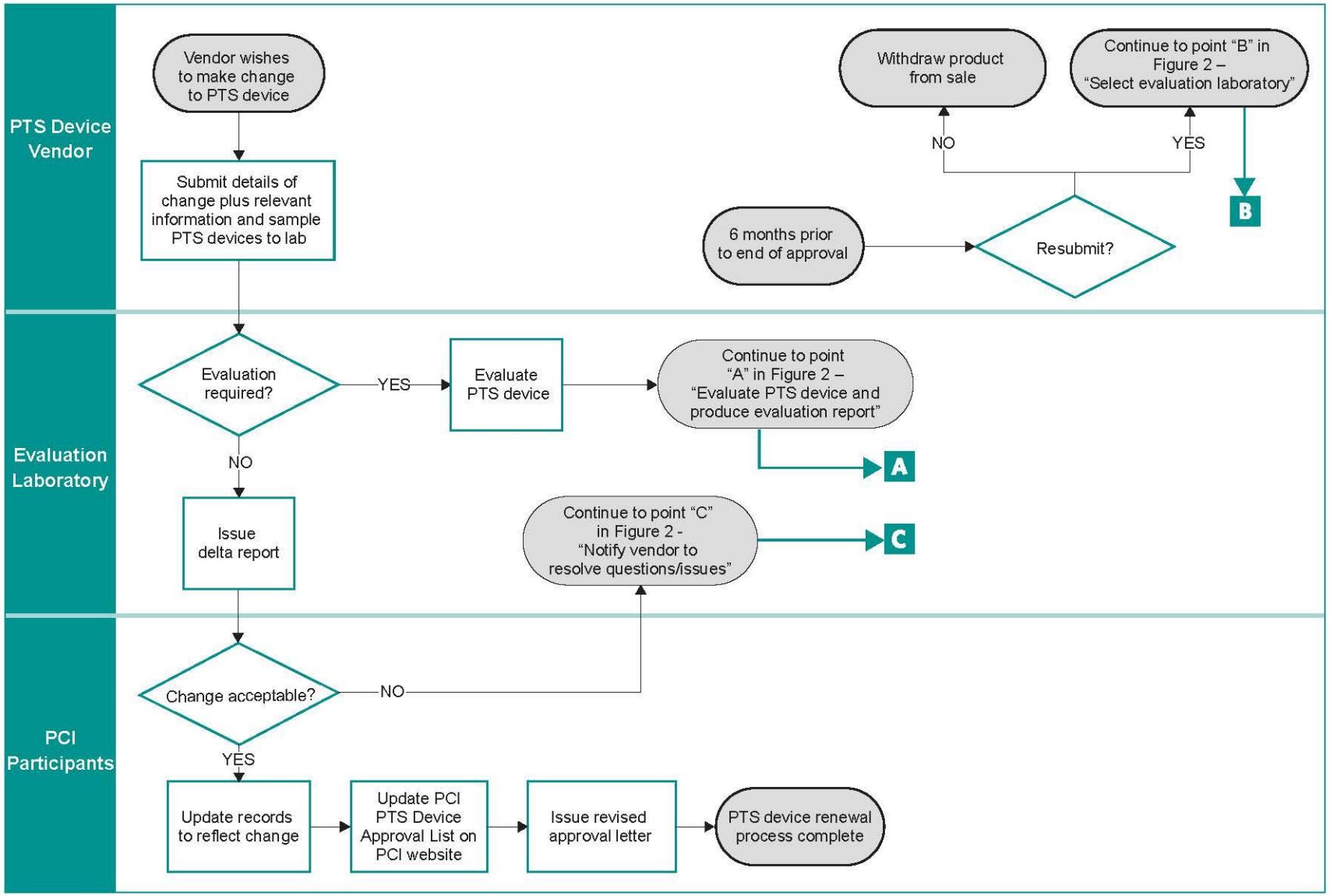
Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2.6 Figure 2: PTS Device Approval Flow Chart



Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

2.7 Figure 3: PTS Device Change Request and Renewal Flow Chart



Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

3 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 the PTS device is posted as a "PCI approved" payment security device on www.pcisecuritystandards.org; then an approval letter will be issued to the vendor.

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 under evaluation at the time of publication.

Modifications for approved devices, termed "deltas," can occur at any time during the product's approval. 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.

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

Upon publication of a major new release (e.g., 3.x, 4.x, 5.x) there will be a twelve month period of overlap beginning May of the year the newer major version is published. Vendors may choose during that period to submit a device under either version of the security requirements. As of 1 May of the following year the older version of security requirements will only be available for delta evaluations.

In the year the prior requirements are retired from use, any vendor using those requirements for a new evaluation must have the device in evaluation by 1 March of that year and PCI must be notified in writing by each PCI recognized laboratory of the specific devices they have under evaluation. The final laboratory evaluation reports must be received by PCI prior to 1 May of that year. If the devices require changes based upon PCI review of the evaluation reports, those changes may be made after 1 May. However, PCI shall not accept any revised evaluation report subsequent to 30 June of that year.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Applicable to POI devices only:

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

- **Device samples:** Two (2) terminals containing the same keys and applications as those supplied to the PCI-recognized laboratory. This includes all approval classes. For large items, please notify via contact details below before shipping. Provision of device samples is a necessary part of a device's approval. These will be securely retained and may be used to assess vulnerability to new attack techniques. If a model is ever compromised in the field, the retained samples may be used to investigate any compromise or security breach.
- **Robust side-channel testing** is an important part of device assessment. Relevant side-channel test data (digitally represented waveforms and associated numerical data) produced by an evaluation must be stored by the laboratory for at least four years following device approval. The Council shall request some or all of this data to be provided as necessary. Laboratories should communicate with the Council to resolve any questions on this matter.
- **Robust logical-anomalies testing** is an important part of device assessment. Relevant fuzzing data examples (output data and/or logs, reports, etc.), providing a representative and comprehendible summary of the fuzzing attack test runs must be presented within or accompanying evaluation reports, indicating what testing was performed and why, in sufficient detail to explain testing rationale and conclusions.

Send devices to:	**Shipping contact information:**
Attn: MasterCard Global Products and Solutions MasterCard Worldwide 5 Booths Park Chelford Road Knutsford Cheshire WA16 8QZ UK	Contact: Mrs. Deborah Corness Telephone: +44 (0)1565 626600 Fax: +44 (0)7738 202 663 E-mail: deborah_corness@mastercard.com

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

4 Preparation for Testing

4.1 Laboratory Services

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

- Guidance on designing payment security devices to conform to the 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.

4.2 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 "PTS Approved Devices" section.

4.3 Test 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.

4.4 Requirements for Testing

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

The 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.

4.5 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

4.6 Testing Timeframes

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

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

4.7 Test Cycle Definition

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

4.8 Technical Support throughout Testing

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

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

5 PCI Fees

Vendors are assessed a fee for every new evaluation report received. In addition, vendors will be assessed an annual listing or maintenance fee for each existing PCI approval. These fees are stipulated at www.pcisecuritystandards.org/fees.

5.1 Delinquencies

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

5.2 New Evaluations

The fee for new evaluations will be a pass-through fee 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.

5.3 Initial Evaluations under Major Versions

All initial evaluations under a major version (e.g., 3.x, 4.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., 3.x—to an approval under another major version number, e.g., 4.x.

5.4 Approval-Listing Fee

The approval-listing fee will be billed semi-annually by PCI SSC. The billing dates shall be set as May 1 and November 1 of every year. Vendors will be billed the full amount for all unexpired PCI approvals existing on April 30 to cover the period May 1 through April 30. The November 1 billing will cover any new listings that post from May 2 through October 31. Vendors with new listings posted during this period will be issued a pro-rated invoice based on the effective date of the listing.

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 1 May. Vendors shall not be billed the annual listing fee for “End of Life” (EOL) products for which they have notified PCI in writing ninety (90) days prior to the billing date of 1 May. An End of Life product is a product no longer marketed for new deployments. This applies only to an entire approval, and not individual items within an approval. The notification should be accompanied by a copy of the end-of-life notification sent by the vendor to their customers. 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

6 Approval Process

6.1 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 *Payment Card Industry 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.

6.2 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.

6.3 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 post the approval information to the website and issue an approval letter. If questions or issues are identified and sent to the laboratory, the cycle resets to one week (seven calendar days) after receipt of a complete and acceptable response from the laboratory. The seven-day reset start does not occur until receipt of an acceptable response for the last open item previously identified. Should additional questions or issues arise, the cycle repeats until a satisfactory response is received, at which time PCI SSC will post the information to the PCI SSC website and issue the approval letter.

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 post the revised information to the website and issue a revised approval letter unless issues or questions arise in a manner similar to the aforementioned. Delta reports are prepared using the major 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

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

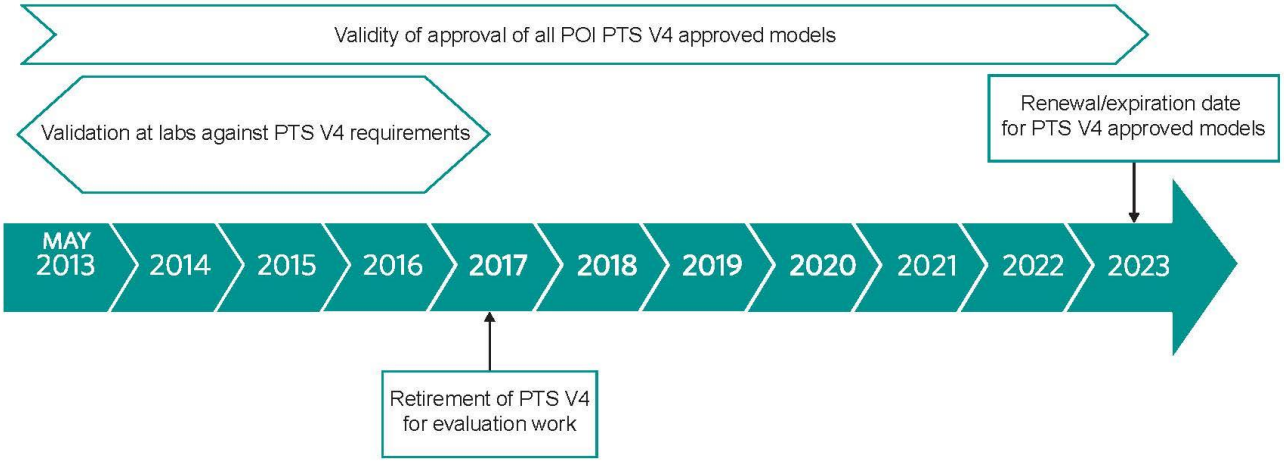
6.4 Listing Delay

Vendors may choose to delay listing a newly approved device for up to a maximum of six months. Written notification to PCI SSC must be submitted through the applicable laboratory along with the evaluation report. In addition, the lab must make a notation in the "Notes" section of the Lab Report Portal indicating the period of time the device listing should be withheld.

6.5 Expiry of Approval

In order to maintain the approval of a given approved model, the vendor must have the approved device model re-evaluated against the current version of the 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.



Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

7 Changes to a Previously Approved PTS Device

If an approved payment security device has undergone changes that may potentially affect security, and/or if the vendor wants the information in its *POI Approval Letter* or *HSM Approval Letter* and on the 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.

7.1 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:

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

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

   If changes to the device 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.)

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

7.2 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.

7.3 Rebranding/Licensing

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, 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.

7.4 Approval Withdrawal

Vendors may submit a request in writing for the withdrawal by PCI SSC of an approval where the vendor has never sold any devices of a specific, previously approved model. This is at the model-name/identifier level, and does not apply to individual hardware or firmware versions. The request must be made using the PTS Administrative Change Request form via one of the PCI-recognized test laboratories. This form is available via the laboratories or the PTS Program Manager pcipts@pcisecuritystandards.org.

7.5 Administrative Changes

Vendors who have undergone a legal name change and desire their approval listings to be updated accordingly must submit a PTS Administrative Change Request form via a PTS-recognized test laboratory. The vendor must also submit a new Vendor Release Agreement under the new company name. If the appearance of the device will change to reflect a new name (labels or faceplate), a delta report must be issued via one of the laboratories.

Vendors who wish to change a model name of an approved device must also use the PTS Administrative Change Request form. However, if any devices have been sold under the prior model name, both names will be listed. Furthermore, images for the device used on the www.pcisecuritystandards.org website must include both the prior and new models.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

8 Notification Following a Security Breach or Compromise

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

8.1 Notification and Timing

Notwithstanding any other legal obligations the vendor may have, the vendor must immediately notify 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.

8.2 Notification Format

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

8.3 Notification Details

Following 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 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

8.4 Actions following a Security Breach or Compromise

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

- Notify 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 Vendor Release Agreement*, using PCI-recognized laboratories to identify the cause of the compromise.

8.5 Withdrawal of Approval

PCI SSC reserves the right to withdraw approval of 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 Vendor Release Agreement.*

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

9 Legal Terms and Conditions

PCI SSC's approval applies only to payment security devices that are identical to the payment security device tested by a 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 approval letter—then the payment security device model should not be considered approved, nor promoted as approved. For example, if a payment security device contains firmware, software, or physical construction that has the same name or model number as those tested by the laboratory, 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

10 Glossary of Terms and Acronyms

Term	Definition
Approval Class	The approval class describes which evaluation requirements the approved device has been tested against. See Appendix A.
Device	Payment device; may be part of a terminal.
EPP	Encrypting PIN pad; approval class, designating embeddable (OEM) devices to be integrated into a cardholder-operated terminal. See Appendix A.
Evaluation Framework	Set of requirements for vendors, test methodology for laboratories, approval process for products, and approval list pertaining to a given payment security device type (POI device, HSM).
HSM	Hardware security module; approval class aimed at devices supporting a variety of payment processing and cardholder authentication applications and processes. See Appendix A.
Hybrid Reader	A device that incorporates capabilities for the capture of card data from either a magnetic-stripe card or an integrated-circuit card (aka a smart or chip card)
ICCR	Integrated-circuit card reader.
KLD	Key-Loading Device
MSR	Magnetic-stripe reader.
OEM	Original equipment manufacturer.
Payment Security Device	Any complete device (for example, a consumer-facing PIN-acceptance device or an HSM) whose characteristics contribute to the security of retail electronic payments or other financial transactions
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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Term	Definition
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
RAP	Remote Administration Platform for HSMs.
Terminal	Commercial device with a business function. It may be dedicated to payment (POS terminal with integrated or separate PIN pad) or to product-dispensing (for example, an ATM or petrol-dispensing self-service).
Test Cycle	Completion of all applicable test procedures performed on a single version of the vendor's payment security device.
UPT	Unattended payment terminal; approval class, designating cardholder-operated payment devices (self-service) that read, capture, and transmit card information in conjunction with an unattended self-service device. See Appendix A.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix A: Device Listing on PCI SSC Website

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

A.1 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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.2 Hardware Security Module (HSM)

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

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

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

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

A.3 Devices with Expired Approval

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.4 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:

- Vendor Name
- Model Name/Number,
- 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 Point of Interaction Device Identifier or the Hardware Security Module Identifier.

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

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

The Device identifier will be included in the approval letter and on the 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.

A.5 Model Name/Number

The model name/number cannot contain any variable characters. All devices within a device family that are intended to be marketed under the same approval number must be explicitly named, and pictures of those devices presented in both the evaluation report and for display on the approval listing.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.6 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.

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.

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 4: 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).

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.7 Security Policy

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

A.8 Approval Number

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

A.9 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 self-contained OEM products that are "bolt on" or drop in type modules (i.e. fully functional PED modules integrating all required components) for UPTs may choose to partner with final form factor vendors of those UPTs (e.g., automated fuel dispenser or kiosk vendors). The OEM vendor's product may meet most of the overall UPT security requirements and the OEM vendor may submit that product in conjunction with additional information from the final form factor vendor on behalf of that vendor, such as AFD or kiosk case design, to the laboratory for evaluation as an UPT.

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.10 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 5: Approval Class Descriptions

Approval Class	Description	Potential Features *(see Table 7 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 products.	▪ Display ▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology ▪ ICCR ▪ MSR ▪ CTLS ▪ SRED ▪ OP
EPP	An approval class aimed at secure PIN entry and encryption modules in an unattended PIN-acceptance device. An EPP may have a built-in display or card reader, or rely upon external displays or card readers installed in the unattended device. An EPP is typically used in an unattended PIN-acceptance device for PIN entry and is controlled by a device controller. An EPP has a clearly defined physical and logical boundary and a tamper-resistant/responsive or tamper-evident shell. At a minimum, a device submitted for EPP approval must contain a PIN-entry keypad along with its built-in secure cryptographic module. Original equipment manufacturers (OEMs) or providers of encrypting PIN pads (EPPs) to unattended PIN-acceptance device manufacturers (e.g., ATMs or UPTs) and other self-service device types can submit 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.	▪ Display ▪ PIN support ▪ Prompt control ▪ Key management ▪ PIN-entry technology ▪ ICCR ▪ MSR ▪ CTLS ▪ SRED ▪ OP

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Approval Class	Description	Potential Features *(see Table 7 below for detail)*
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
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.	Display PIN support Prompt control Key management PIN-entry technology ICCR MSR CTLS SRED OP
KLD	An SCD that may be used for securely receiving, storing, and transferring data between compatible cryptographic and communications equipment. Key-transfer and loading functions include the following: ▪ Export of a key from one secure cryptographic device (SCD) to another SCD in plaintext, component, or enciphered form; ▪ Export of a key component from an SCD into a tamper-evident package (e.g., blind mailer); ▪ Import of key components into an SCD from a tamper-evident package; Temporary storage of the key in plaintext, component, or enciphered form within an SCD during transfer.	N/A
RAP	This is for platforms that are used for remote administration of HSMs. Such administration may include device configuration and key-loading services.	N/A

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Approval Class	Description	Potential Features *(see Table 7 below for detail)*
Non-PED	An approval class of POI devices that does NOT allow the entry of a PIN for a payment card transaction, This class is for ALL POI devices or device combinations, attended or unattended, which do not support PIN-based payment transactions. OEM product types may require further integration into a POI terminal. The device or any combination of hardware can be used as evaluated to operate in an acquirer network. The firmware must include an acquirer-approved payment application necessary for its operation. Non-PED POI devices intended for use in an attended environment must be self-contained, fully functional units that are capable of processing payment transactions, and must include a merchant interface necessary for their operation. Non-PED POI devices (terminals) are validated to the Secure Reading and Exchange of Data Module and, if applicable, the Open Protocols Module. These non-PED POI devices are NOT approved for PIN acceptance.	ICCR MSR CTLS SRED OP

A.11 Version

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

A.12 Expiry Date

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

Table 6: Approval Expiry Dates

Requirements Version Used During Evaluation At Laboratory	Expiration of Requirements	Approval Expiration Of Device Models
Version 5.x of *PCI PTS POI Security Requirements*	April 2020	April 2026
Version 3.x of *PCI HSM Security Requirements*	April 2020	April 2026
Version 4.x of *PCI PTS POI Security Requirements*	September 2017	April 2023
Version 2.x of *PCI HSM Security Requirements*	June 2017	April 2022
Version 3.x of *PCI PTS POI Security Requirements*	April 2014	April 2020
Version 1.x of *PCI HSM Security Requirements*	April 2013	April 2019
Version 2.x of *PCI PED or EPP Security Requirements*	April 2011	April 2017
Version 1.x of *PCI UPT Security Requirements*	April 2011	April 2017
Version 1.x *PCI PED* or *EPP Security Requirements*	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.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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*

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

A.13 Specific Features per Approval Class

Table 7: Specific Features

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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) or AES for PIN encryption for online PIN.TDES requires use of at least a double-length key. A MK/SK (master key, session key), DUKPT, and/or Fixed designation denote that the device has been evaluated successfully to support the implementation of TDES for that particular key-management 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.* Where AES is used, that will be noted in conjunction with the MK/SK or Fixed methodologies.
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. ▪ **N/A:** For HSMs, Non-PEDs, and for SCRs except as denoted in the SCR approval class
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. The use of a device with components (e.g., EPPs, card readers) that are different than that listed as an approved component for that device invalidates that device's approval.

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Feature and Applicability	Description
Functions Provided (PED, EPP, UPT, SCR, Non-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) or Contactless (CTLS). ***Note:*** *Contactless readers are only considered compliant for P2PE usage if the Approval Class in question has been validated to SRED. Furthermore, some device approvals may have versions validated to SRED and some that are not. Where such a mix occurs, only devices using a firmware version designated for SRED are validated to meet the contactless reader security requirements. For devices with contactless readers using firmware that is not validated to SRED, the contactless readers are not validated to any security requirements.* ▪ **Display:** The device has an integrated display used for cardholder prompts and possibly the presentation of other information. ▪ **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.
Additional Information	This field may be used to place any additional pertinent information. For example, when a vendor has changed the status of a device to end-of-life as delineated in *Section 4.3 – Fees.* and thus the device is no longer available for purchase except for maintenance purposes subject to payment brand rules. This will also be used for v2 HSMs to delineate whether they are approved for restricted or unrestricted usage as delineated in the HSM Security Requirements: ▪ **Restricted –** Approval is valid only when deployed in Controlled Environments or more robust (e.g., Secure Environments) as defined in ISO 13491-2 and in the device's PCI HSM Security Policy. ▪ **Unrestricted –** Approval is valid in any environment.
Device Form Factor	All security-relevant components (PIN pad, display, card reader(s)) of the device are shown in one or more pictures. At least one of the pictures must fulfill the requirement that the hardware version number must be shown on a label attached to the device. Note that for devices with multiple approved hardware versions, only one such illustration is necessary to facilitate purchasers of these devices recognizing how to determine the approved version(s).

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Delta Evaluations – Scoping Guidance

B.1 Introduction

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

This appendix is meant to provide guidance on whether changes made by vendors to a validated PTS device (whether POI or HSM) are limited enough in scope such that it is permissible that said changes to the validated PTS device may be assessed as a "delta" to the original validation.

B.2 What is a Delta Evaluation?

All initial evaluations under a major version (e.g., 1.x, 2.x, 3.x. 4.x, etc.) of the security requirements for a given product shall constitute a new evaluation and shall receive a new approval number.

Revisions to approved devices are termed "deltas." Delta reviews involve the Recognized PTS Laboratory (or "PTS Lab") assessing the changes based upon the most current major version of the security requirements used for the original assessment and the most current FAQ publication associated with those requirements. For example, if a device was originally assessed against PTS POI v4.0, any delta assessments would have to be performed using v4.1 (the most current version of PTS v4.x and the last issued v4.x FAQs). Examples of deltas include:

- Revisions to existing firmware or hardware on previously approved devices to add or modify functionality;
- Adding EMV Level 1 to an existing approval;
- Maintenance fixes on devices that have expired approvals;
- Assessment of a device for offline PIN entry where the existing approval is only for online PIN entry, or vice versa;
- The porting of a new set of firmware to an existing approved device.

Delta evaluations are not permitted to take a product previously approved under an earlier major version number of the PTS POI Standard—e.g., 3.x—to an approval under another major version number—e.g., 4.x.

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

B.3 Determining Whether a Delta is Permissible

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

B.3.1 Sample Impacts of Certain Changes

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

B.3.2 Firmware Changes

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

Table 8: Firmware Change Types and Impacted Requirements

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

Firmware Change Types	Impacted Requirements			
	PTS Standard Version			
	v1.x	v2.x	v3.x	v4.x
Any firmware change	N/A	N/A	N/A	B20
Firmware changes with no apparent impact on PCI Requirements	B3	B3	B3, F1, G1, H1, I1	B3, F1
Amendments in secure tamper-recovery methodology	B1	B1	B1	B1
Error handling (i.e., buffer overflows)	A5, B2	A3, B2	A3, B2	A3, B2
Amendments to external communications protocols	B2	B2	B2, F1, G1 H1, I1	B2, F1
Change to software/firmware update mechanisms	B3, B4	B3, B4	B3, B4, J4	B3, B4, B4.1, J4
New firmware/application authentication scheme	B4	B4	B4	B4, B4.1
Amendments to PIN-digit timeouts	B7, C3	B6, B10	B6, B10	B6, B10
Amendments to cryptographic functions	B10, C2, C4, C6, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4	B6, B9, B12, B13, D4
Non-security changes to card-reader firmware	D4	A11, D4	A10, D4	A9, D4
Changes to sensitive service authentication mechanisms	B8, B9	B7, B8	B7, B8	B7, B8
Update key-loading methodology	C5	B11	B11, J4	B11, J4
Amendments to key management	C1, C5, C6, C7, C8	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1	B11, B13, B14, C1, D1

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Firmware Change Types	Impacted Requirements			
	PTS Standard Version			
	v1.x	v2.x	v3.x	v4.x
Change to key hierarchy	C1, C5, C7	B11, C1, D1	B11, C1, D1	B11, C1, D1
Amendments to key storage	C1, C5	B11, D1	B11, D1	B11, D1
New key types	C1, C5, C6	B11, B13, D1	B11, B13, D1	B11, B13 D1
Amendments in PIN-length handling	C4, D4	B12, D4	B12, D4	B12, D4
Minor user interface changes	B5, B6	B5, B15	B5, B15, F1 G1, H1, I1	B5, B15, F1
Updated PIN prompts	A7, B5, B6	A8, B5, B15	B5, B15, B16	B5, B15, B16
Addition of SRED functionality ***Note:*** *SRED deltas on v2.x devices will not be accepted after 31 December 2012.*	N/A	N/A	B17-19, K1-25	B17-19 K1-23

B.3.3 Hardware Changes

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

The inclusion of more than four (4) of the identified hardware change types as delineated in the table below in a single delta submission for a previously approved PTS device may effectively represent a new device that should be subjected to its own full assessment against the latest version of the current PTS Standard. Candidates for delta submissions that surpass this threshold which, in the opinion of the PTS Lab, represent a minor change to the approved PTS device, should be presented to the PCI SSC in advance of completing the assessment to determine whether the scope of change is too great. It is also not acceptable to put forward a series of delta submissions with hardware changes as an attempt to work around this threshold. If delta submissions with hardware changes are received within three months of the approval of the reference device, sufficient information must accompany the submission to justify the need for the change and why it wasn't included as part of the previously approved submission. In all cases, cumulative changes will be considered when assessing the propriety of any specific delta request.

Any change made to the hardware of an approved PED, even to the non-security related components, has the potential to directly or indirectly impact the security of the device. As such, any delta assessment that includes modifications to the approved device's hardware—even the circuitry not related to the security functions of the device—must, at a minimum, be reviewed by the PTS Lab with respect to the potential impact on the following security requirements of the applicable version of the PTS Standard against which the assessment is being performed:

- V1.x: Requirements A1, A2, A3 & C1;
- V2.x: Requirements A1 & A7; and
- V3.x: Requirements A1 & A7 and
- V4x: Requirements A1, A6, B1 & B20

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Table 9: Acceptable Hardware Changes

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

Hardware Change Types	Impacted Requirements			
	PTS Standard Version			
	v1.x	v2.x	v3.x	v4.x
Any hardware change[2]	A1, A2, A3, C1	A1, A7	A1, A7	A1, A6, B2, B20
Changes in casing plastics (e.g., cover-opening dimensions, areas that permit internal access, changes to PED look and feel, etc.) or output-only displays. Amended devices must remain consistent to the device's original form factor.	A4, A7, A9-A11, D1-D4	A2, A6, A8-A11, D1-D4	A2, A6, A8-A11, B16, D1-D4, K1-K3	A5, A7-A9, A11 B16, D1-D4 K1-K3
Modification to tamper/removal switches (e.g., changes to materials, performance, location, circuitry, tamper response, etc.) or tamper-resistance/evidence features	A5, D1	A2, A3, A11, D1	A2, A3, A10, D1	A2, A9, D1
Modifications to the secure controller(s)	A5, A6, A7, A9, B1-B10, C2-C8, D4	A3, A4, A6, A8, B1-B15, C1, D4	A3, A4, A6, A8, A11, B1-B19, C1, D4	A3, A4, A5, A7, A10, B2-B19, C1, D4
Changes to user interfaces that could be used for PIN entry (e.g., touch screens, keypad membranes, etc., but excluding modifications of function keys)	A5, A7, A9, D1	A2, A6, A8, A9, A11, D1	A2, A6, A8-A10, B16, D1	A5, A7-A9, A11, B16, D1
Replacement or addition of any component card reader and/or ICCR	D1-4	A10, A11, D1-4	A10, D1-D4, K1, K2	A9, D1-D4 K1-K2
Modifications to communications circuitry	A5, B2, D1	A2, A3, B2, D1	A2, A3, B2, D1, F1, G1 H1, I1	A3, B2, D1, F1
Modifications to power circuitry	A5	A3	A3	A3
Modifications to other major components of the PCB circuitry (e.g., audio circuitry, heater circuitry, etc.). This excludes re-routing of circuits.	A5, A8	A3, A5	A3, A5	A3, A11

[2] This item is not to be included in the count of changes when determining whether the number of changes in a single delta submission is within the acceptable range of four (4).

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

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

B.5 Delta Documentation Requirements

B.5.1 Reporting Guidance for PTS Vendors

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

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

B.5.2 Reporting Requirements for PTS Laboratories

PTS Labs must provide the following documentation with each delta submission:

- A high-level description of the changes that have been made to the approved PTS device;
- Citations of:
  - The reference approval report and any subsequent delta submissions upon which the current delta submission is based; and
  - Any supporting documentation used to substantiate the findings represented in the delta submission;

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

B.6 Applicability of FAQs During Delta Assessments

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

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

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

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

B.7 Considerations for Updated Components in Integrated Terminals

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

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

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: PTS Administrative Change Request

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

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

Description of Change(s)				
Type of Change (check all that apply)	☐ Business Name	☐ Business Address	☐ Device Model Name(s)	☐ Contact Name/Address
Briefly describe reason for change(s)				

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

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

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.

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

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

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

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

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

Supporting Documentation Required

	Administrative Change (this form)	**Security Policy**	**Vendor Release Agreement (VRA)**	**Device Images***
Company Name Change	X	X	X	X
Device Model name	X	X		X
Primary Contact Name	X			

** If applicable images must be submitted via a delta submission.*

Copyright © 2010-2016 PCI Security Standards Council, LLC. All Rights Reserved.