



Payment Card Industry (PCI) Unattended Payment Terminals (UPT)

Derived Test Requirements

Version 1.0

April 2009

© PCI Security Standards Council LLC 2009

This document and its contents may not be used, copied, disclosed, or distributed for any purpose except in accordance with the terms and conditions of the Non-Disclosure Agreement executed between the PCI Security Standards Council LLC and your company. Please review the Non-Disclosure Agreement before reading this document.

Document Changes

Date	Version	Description
March 2006	0.2	Initial Draft based on Version 0.2 of the UPT Requirements.
April 2006	0.3	Updated according to Version 0.3 of the UPT Requirements
July 2006	0.5	Updates to replace cost with Attack potential, and include case replacement as part of A1.1 and reorder requirements to match with POS UPT. Match format and numbering scheme with the POS UPT DTR. Simplify Document structure
October 2006	0.61	Alignment with the draft version 2.0 of the PCI POS UPT requirements,
April 2007	0.70	Incorporated Vendor comments
May 2007	0.71	Alignment with the final 2.0 versions of the PCI POS UPT and PCI EPP requirements
April 2008	0.72	Harmonize with PCI UPT
November 2008	0.75	PWG/Lab meeting changes
April 2009	1.0	Initial Release

Table of Contents

Document Changes	iii
Introduction vi	
Core Derived Test Requirements – Physical.....	1
DTR A1.1 Tamper-Detection Mechanisms.....	1
DTR A1.2 Independent Security Mechanisms.....	3
DTR A2 Response to Internal Access	4
DTR A3 Robustness Under Changing Environmental and Operational Conditions	6
DTR A4 Protection of Sensitive Functions or Information	7
DTR A5 Audible Tones During PIN Entry	8
DTR A6 Monitoring During PIN Entry	9
DTR A7 Determining Keys Analysis	10
DTR A8 Protection against Removal.....	11
DTR A9 Visual Observation Deterrents.....	13
DTR A10 Protection Against Card Trapping.....	14
DTR A11 Magnetic-Stripe Reader.....	15
Core Derived Test Requirements – Logical.....	16
DTR B1 Self-Test	16
DTR B2 Logical Anomalies.....	17
DTR B3 Firmware Certification.....	18
DTR B4 Firmware Updates	19
DTR B5 Differentiation of Entered PIN	20
DTR B6 Clearing of Internal Buffers	21
DTR B7 Protection of Sensitive Services	22
DTR B8 Sensitive Services Limits	24
DTR B9 Random Numbers.....	25
DTR B10 Exhaustive PIN Determination.....	26
DTR B11 Key Management.....	27
DTR B12 Encryption Algorithm Test.....	32
DTR B13 Encryption or Decryption of Arbitrary Data Within the Device	33
DTR B14 Clear-Text Key Security	34
DTR B15.1 Prompts Under Control of the Cryptographic Unit	35
DTR B15.2 Altering User Interface Prompts Cost Analysis.....	37
DTR B15.3 User Interface Consistency.....	38
DTR B16 Application Separation.....	40
DTR B17 Minimal Configuration	41
DTR B18 Control of any Numeric Interface	42
Online Derived Test Requirements	43
DTR C1 Key Substitution.....	43

Offline Derived Test Requirements	44
DTR D1 Penetration Protection	44
DTR D2.1 ICC Reader Slot Geometry.....	45
DTR D2.2 ICC Reader Slot Visibility.....	46
DTR D3 ICC Reader Construction (Wires)	47
DTR D4 PIN Protection During Transmission Between UPT and ICC Reader	48
Appendix A: Criteria for the Privacy Screen Design	51
A.1 Privacy Screen Design Criteria to be Met by the UPT's Design	51
A.2 Privacy Screen Design Criteria to be Met by the UPT's Installed Environment	55
Appendix B: Attack Potential Formula (Adopted from JIL).....	57
Appendix C: Configuration and Use of the sts Tool	63

Introduction

The Test Requirements in this document were derived from the PCI POS PIN Entry Device (UPT) Security Requirements as embodied in the *PCI POS PIN Entry Device Security Requirements* manual. These Derived Test Requirements (DTRs) are grouped into four sections within this document:

- Core Physical Security Derived Test Requirements,
- Core Logical Security Derived Test Requirements,
- Additional Online Derived Test Requirements, and
- Additional Offline Derived Test Requirements

Each PCI requirement as stated in the *PCI Unattended Payment Terminal Security Requirements* manual is represented by a subsection. For example, Requirement A1.1 is represented in this document as:

DTR A1.1 Tamper-Detection Mechanisms

When appropriate, each PCI requirement has been divided into component parts. These parts are identified by the corresponding PCI requirement number and a number distinguishing it from other components of the same requirement.

For example, the first component under the section for DTR A.1.1 is:

A1.1.1

DTRs are provided under each of these components. These are identified by a “T,” followed by the component identification number, which is followed by a number that distinguishes it from the other DTRs of the same component.

Core Derived Test Requirements – Physical

DTR A1.1 Tamper-Detection Mechanisms

The UPT uses tamper-detection and response mechanisms that cause the UPT to become immediately inoperable and results in the automatic and immediate erasure of any secret information that may be stored in the UPT, such that it becomes infeasible to recover the secret information. These mechanisms protect against physical penetration of the device by means of (but not limited to) drills, lasers, chemical solvents, opening covers, splitting the casing (seams), and using ventilation openings; and there is not any demonstrable way to disable or defeat the mechanisms and insert a PIN-disclosing bug or gain access to secret information without requiring an attack potential of at least 25 per UPT, exclusive of the ICC reader for identification and initial exploitation as defined in Appendix B of PCI UPT DTRs.

Guidance

The objective of this section is to assess the UPT's ability to protect clear-text PINs and other sensitive data. Attack scenarios must be in support of the compromise of clear-text PINs and other sensitive data as noted in A1.1.

Requirement A7 focuses on determination of secret or private keys. This requirement focuses on tamper-detection and response mechanisms in place to prevent PIN disclosure.

"Immediate" is defined as fast enough to ensure erasure occurs before the tamper-detection mechanisms can be disabled using attack methods described in A1.1.

For those devices that do not contain secret information, device disablement may be used in lieu of "immediate erasure of all secret information"

"Secret information" is any private or secret cryptographic keys or passwords that the UPT relies on to maintain security characteristics governed by PCI requirements. If any of these keys are not zeroized, then other mechanisms must exist to disable the device and these keys must be protected in accordance with Requirement A7.

Secret or private cryptographic keys that are never used to encrypt or decrypt data; or are not used for authentication, do not need to be considered secret data, and therefore do not need to be erased—e.g., where the device uses a chip set that automatically generates keys at initialization but the keys are not subsequently used by the device.

When designing an attack against the UPT as part of A1.1, replacement of casing parts like the front and rear case of the EPP shall be considered as part of the overall attack.

- TA1.1.1** The tester shall visually inspect the tamper-detect mechanism to verify the assertions provided by the vendor in response to Section A1.1 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the tamper-detection mechanism.
- TA1.1.2** The tester shall examine additional relevant documentation, such as schematics and assembly drawings, submitted by the vendor to verify that it supports the vendor responses.

- TA1.1.3** The tester shall open the UPT to activate the tamper-detection mechanisms and then perform tests to support evidence that the UPT is no longer operational. The tester shall then perform tests to support evidence that keys and secret data have been erased or are otherwise non-recoverable. Tests that may be performed could include attempting a transaction to determine if the transaction fails, using a special function of the UPT that allows a user to determine the status of secret data, or using special software to determine if secret data has been erased.
- TA1.1.4** The tester shall examine the response to Section A1.1 of the *PCI UPT Evaluation Vendor Questionnaire* relating to response of the EPP to tamper detection, for consistency.
- TA1.1.5** The tester shall examine vendor-supplied documentation to determine if the UPT employs active or passive (i.e., removal of power) erasure. If the UPT employs passive erasure, the tester shall verify that erasure occurs rapidly enough to prevent an attacker from opening the UPT and stopping erasure before it is effective. The tester may create an attack scenario, which may be performed in its entirety or in part to verify the theory.
- TA1.1.6** The tester shall develop attack scenario(s) to disable or defeat the tamper-detection mechanisms and insert a PIN-disclosing bug or gain access to secret information, which requires an attack potential of <25 per UPT. The attack potential value shall be based on the scheme depicted in Appendix B.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR A1.2 Independent Security Mechanisms

Failure of a single security mechanism does not compromise UPT security. Protection against a threat is based on a combination of at least two independent security mechanisms.

Guidance

In general, techniques may include any combination of tamper-detection methods. Security mechanisms must not rely on insecure services or characteristics provided by the UPT such as (but not limited to) its power supply and unprotected wires. Tamper-evident labels and similar methods involving tamper evidence are not considered a security mechanism.

This requirement does not imply the need for redundant security mechanisms.

- TA1.2.1** The tester shall examine the response to Section A1.2 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A1.2 of the *PCI UPT Security Requirements* manual for consistency relevant to DTR A1.2. The vendor responses should clearly indicate that the failure of a single security mechanism does not compromise UPT security.
- TA1.2.2** The tester shall examine any additional relevant documentation, such as assembly drawings, submitted by the vendor to verify that it supports the vendor responses.
- TA1.2.3** The tester shall verify that protection against a threat is based on a combination of at least two independent security mechanisms.

DTR A2 Response to Internal Access

If the UPT or its components permit access to internal areas (e.g., for service or maintenance), then it is not possible using this access area to insert a PIN-disclosing bug. Immediate access to such sensitive data such as PIN or cryptographic data is either prevented by the design of the internal areas (e.g., by enclosing components with sensitive data into tamper-resistant/responsive enclosures), or it has a mechanism so that access to internal areas causes the immediate erasure of sensitive data.

Guidance

The ICC reader may consist of areas of different protection level: the areas of the IC card itself and the area holding retracted cards.

"Immediate" is defined as fast enough to ensure erasure occurs before the tamper-detection mechanisms can be disabled using attack methods described in A1.1.

Secret or private cryptographic keys that are never used to encrypt or decrypt data, or are not used for authentication, do not need to be considered sensitive data and therefore do not need to be erased—e.g., where the device uses a chip set that automatically generates keys at initialization but the keys are not subsequently used by the device.

- TA2.1** The tester shall examine the response to Section A2 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A2 of *PCI UPT Security Requirements* for consistency relevant to A2.
- TA2.2** The tester shall examine any relevant documentation, such as assembly drawings, submitted by the vendor to verify that it supports the vendor responses.
- TA2.3** The tester shall identify the UPT components applicable to this requirement.
- TA2.4** The tester shall verify the existence and design of any mechanisms asserted by the vendor to protect any physical access ports and/or to prevent immediate access to sensitive information like PIN and cryptographic data. This will be accomplished by disassembling the device and examining the mechanisms.
- TA2.5** For each of the applicable UPT components, the tester shall attempt to remove the access cover by disabling or defeating the tamper-detection mechanisms. To remove the cover the tester may open, pry, or otherwise disassemble the components at the cover seams and remove other plates, connectors, etc. to gain access to the tamper-detection mechanisms. Removal shall not consist of drilling, milling, burning, melting, grinding, or dissolving the cover or enclosure. The tester may drill out visible fasteners (e.g., screws, rivets, press-fittings, etc.) to remove the cover.
- TA2.6** The tester shall verify that attempts to remove the cover by removing fasteners, plates, connectors, etc. or by creating a gap between the covers or cover and housing does not allow access to probe critical security circuitry without triggering the tamper-detection mechanisms.
- TA2.7** The tester shall open the components to activate the tamper-detection mechanisms, and then perform tests to support evidence that keys and secret data have been erased. Tests that may be performed could include attempting a transaction to determine if the transaction fails, using a special function of the component that allows a user to determine the status of secret data, or using special software to determine if secret data has been erased.

- TA2.8** The tester shall examine vendor-supplied documentation to determine if the components employ active or passive (i.e., removal of power) erasure. If the components employ passive erasure, the tester shall verify that it occurs rapidly enough to prevent an attacker from opening the UPT and stopping erasure before it is effective. The tester may create an attack scenario which may be performed all or in part to verify the theory.

DTR A3 Robustness Under Changing Environmental and Operational Conditions

The security of the UPT is not compromised by altering environmental conditions or operational conditions (for example subjecting the UPT to temperatures or operating voltages outside the stated operating ranges).

Guidance

The vendor must either provide substantive data to support the security of the product outside normal operating conditions, or show that the product uses sensors that will trigger a tamper response.

The objective is not to replicate the vendor testing, but instead it is to account for shortcomings within the vendor's implementation.

TA3.1 The tester shall examine the response to Section A3 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A3 of the *PCI UPT Security Requirements manual* for consistency relevant to Requirement A3. The vendor responses should clearly state that the security of the UPT is not compromised by altering environmental conditions or operational conditions.

TA3.2 The tester shall examine any additional relevant documentation, such as schematics, data sheets, vendor test procedures and test reports, etc. submitted by the vendor to verify that it supports vendor responses. This may include data provided to support Requirement B2 under different environmental conditions.

TA3.3 The tester shall verify that the vendor's stated measures protect against the compromise of the UPT by altering either environmental conditions or operational conditions, and assess the adequateness of the vendor test procedures and reports.

TA3.4 The tester shall develop attack scenarios to compromise the UPT by altering environmental and or operational conditions.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR A4 Protection of Sensitive Functions or Information

Sensitive functions or information are only used in the corresponding protected area(s) of the UPT. Sensitive information and functions dealing with sensitive information are protected from modification without requiring an attack potential of at least 25 per UPT, exclusive of the ICC Reader, for identification and initial exploitation as defined in Appendix B.

Guidance

Public keys used for functions that impact security requirements, such as firmware updates, display prompt control, or remote key distribution schemes must be protected against modification and substitution. Secret and private keys used for functions that impact security requirements must be protected against modification, substitution or disclosure.

- TA4.1** The tester shall examine the response to Section A4 of the PCI UPT Evaluation Vendor Questionnaire and the response to Requirement A4 of the PCI UPT Security Requirements Manual for consistency relevant to Requirement A4. The vendor responses should clearly indicate what sensitive information and functions exists; and that sensitive functions or information are only used in the protected area(s) of the UPT; and that sensitive information and functions dealing with sensitive information are protected from modification.
- TA4.2** The tester shall examine any additional relevant documentation, such as assembly drawings and functional specifications submitted by the vendor to verify that it supports the vendor responses.
- TA4.3** Verify the completeness of the information regarding sensitive information and functions presented by the vendor.
- TA4.4** The tester shall develop attack scenarios to defeat or circumvent the protection mechanisms dealing with sensitive information and functions, using attack scenarios, with an attack potential of < 25 per UPT, for identification and initial exploitation. The cost calculation shall be based on the scheme depicted in Appendix B.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR A5 Audible Tones During PIN Entry

If the PIN entry is accompanied by audible tones, then the tone for each entered PIN digit is indistinguishable from the tone for any other entered PIN digit.

- TA5.1** The tester shall examine the vendor's response to Section A5 of the PCI UPT Evaluation Vendor Questionnaire and the response to Requirement A5 of the PCI UPT Security Requirements for consistency relevant to A5.1.
- TA5.2** The tester shall examine any additional information (i.e., specifications, schematics, block diagrams, etc.) that contains information on tone generation during PIN entry to determine if it supports the assertions made by the vendor.
- TA5.3** The tester shall verify that any audible tones accompanying PIN entry are indistinguishable e.g., by listening to the tones while entering a PIN number or by otherwise analyzing or measuring the tone/tone-generation circuitry.

DTR A6 Monitoring During PIN Entry

There is no feasible way to determine any entered and internally transmitted PIN digit by monitoring sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring, even with the cooperation of the terminal operator without requiring an attack potential of at least 25 per UPT to defeat or circumvent for identification and initial exploitation as defined in Appendix B

Guidance

For A6 monitoring sound refers to other audible sounds apart from the beep generated by the UPT when a key is pressed.

Monitoring is to be done outside of the protected area of the UPT (in most cases: outside the EPP).

- TA6.1** The tester shall examine the vendor's response to Section A6 of the PCI UPT Evaluation Vendor Questionnaire and the response to Requirement A6 of the PCI UPT Security Requirements for consistency relevant to A6.
- TA6.2** The tester shall examine any relevant documentation, such as schematics and assembly drawings, submitted by the vendor to verify that it supports the vendor responses to the PCI UPT Evaluation Vendor Questionnaire.
- TA6.3** The tester shall visually inspect the UPT to verify the assertions provided by the vendor in the PCI UPT Evaluation Vendor Questionnaire relating to protections against the monitoring of sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring. This could include verifying that any components that provide protection are as stated by the vendor.
- TA6.4** The tester shall perform a sample transaction to verify the assertions provided by the vendor relating to protections against monitoring.
- TA6.5** The tester shall develop attack scenarios to defeat or circumvent the protection mechanisms against the monitoring of sound, electro-magnetic emissions, power consumption or any other external characteristic available for monitoring, using attack scenarios which require an attack potential of <25 per UPT for identification and initial exploitation. The cost calculation shall be based on the scheme depicted in Appendix B.

Monitoring must be done outside the protected areas of the UPT components (like the EPP or ICC reader) and address the transmission inside these UPT components.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR A7 Determining Keys Analysis

To determine any PIN-security-related cryptographic key resident in the UPT by penetration of the UPT and/or by monitoring emanations from the EPP or ICC reader (including power fluctuations), requires an attack potential of at least 35 for identification and initial exploitation as defined in Appendix B.

Guidance

The vendor may need to supply specific test software to the evaluation laboratory to enable rigorous side channel attack analysis to be performed.

Keys resident in the UPT or its components means plaintext secret or private keys. If the encrypted keys are protected in accordance with the minimum key sizes and parameters for the key encipherment algorithm(s) used as stipulated in B11, they do not need to be considered.

- TA7.1** The tester shall examine the vendor's response to Section A7 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A7 of the *PCI UPT Security Requirements* for consistency relevant to A7.
- TA7.2** The tester shall examine any relevant documentation, such as assembly drawings, test data, etc., submitted by the vendor to verify that it supports the vendor responses.
- TA7.3** The tester shall develop attack scenarios to determine any PIN-security-related cryptographic key resident in the UPT either by penetration or by monitoring emanations from the UPT. The tester is not required to perform the attack but may perform all or part of the attack to verify its validity. The calculation shall be based on the scheme depicted in Appendix B. If an attack scenario can be developed that yields an attack potential of less than 35 per UPT for identification and initial exploitation as defined in Appendix B, the vendor assertion cannot be verified.

DTR A8 Protection against Removal

The EPP and the ICC reader of the UPT are protected against removal; defeating or circumventing this mechanism must require an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B.

Guidance

The objective of this section is to assess the UPT's ability to protect the EPP and ICC reader against removal from the cabinet. This protection aims against EPP overlays or chained ICC readers; it also aims at complicating attacks against the EPP and ICC reader.

The intent of the requirement to protect the EPP against removal from the cabinet aims against inserting an overlay between the EPP and the casing/cabinet within which the EPP is installed and to hinder the removal of the EPP from its working location for an attack under laboratory conditions.

Installation or removal of an EPP or ICC reader requires an authorized process. An authorized installation must provide traceability and accountability (what happened, when, and who did it).

Protection against removal may be implemented as detection of removal and procedures for authorized installation or re-installation. The procedures must:

- *Use dual-control techniques;*
- *Provide accountability and traceability;*
- *Prevent replay of authorization data; and*
- *Cause the device to not process PIN data until authorized to do so.*

- TA8.1** The tester shall examine the vendor's response to Section A8 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A8 of the *PCI UPT Security Requirements* for consistency relevant to A8.
- TA8.2** The tester shall visually inspect the UPT's EPP and ICC reader to verify the assertions provided by the vendor in response to Section A8 PCI UPT Evaluation Vendor Questionnaire.
- TA8.3** The tester shall examine additional relevant documentation, such as schematics and assembly drawings submitted by the vendor to verify that it supports the vendor responses.
- TA8.4** The tester shall determine whether the device uses passive or active protection, and assess the method for installation and for permanent or temporary removal. Assess the method for installation and full/temporary removal. An option for temporary removal without secret and private key erasure requires an authorized method.
- TA8.5** If the device allows for temporary removal and re-installation, the tester shall verify that:
- The authorization for removal implements the principles of dual control,
 - Sensitive information required for the authorization (e.g. passwords) is initialized or used in a way, that prevents replay at the same or a different device,
 - When removed/substituted without authorization the device will not further process PINs.
 - An authorized installation must provide traceability and accountability

TA8.6 The tester shall develop attack scenario(s) to defeat or circumvent the protection against removal, which require an attack potential of <16 per UPT for identification and initial exploitation. The cost calculation shall be based on the scheme depicted in Appendix B.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR A9 Visual Observation Deterrents

The UPT provides a means to deter the visual observation of PIN values as they are being entered by the cardholder.

Guidance

Some markets may require Option A.1 of Appendix A or a stricter criterion.

- TA9.1** The tester shall examine the vendor's response to Section A9 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A9 of the *PCI UPT Security Requirements* for consistency relevant to A9.
- TA9.2** The tester shall examine the means to deter the visual observation of PIN values provided by the UPT, and/or as described in the UPT documentation, to verify the assertions of the vendor.
- TA9.3** The tester will verify the physical properties of the privacy screen. The privacy screen shall provide protection as described in Appendix A of this document. Alternatively, the vendor may use less restrictive privacy shield criteria provided that the vendor supplies rules and guidance as to how the visual observation is to be deterred by the environment in which the UPT is installed. These rules shall be binding for the organization placing the UPT into the environment, e.g., the acquirer or merchant. If the vendor gives rules for an external physical privacy shield, then the vendor shall provide a demo/sample with the appropriate dimensions. The tester shall examine the information to verify the assertions of the vendor. The tester shall consider the examples included in Appendix A, Section A.2, of this document when evaluating the vendor's visual observation deterrence rules. The user (acquirer or merchant) instructions provided by the vendor shall clearly state the acquirer or merchant must meet the implementation criteria or else deploy UPTs meeting the criteria defined in Appendix A, Section A1.
- TA9.4** If the means to deter visual observation are not an integral part of the EPP, the vendor shall specify by appropriate means (e.g., drawings and description) how the visual observation is deterred by the structure or piece of equipment housing the UPT. These specifications shall be binding for the vendor. The tester shall examine this specification to deter the visual observation of PIN values provided by the UPT to verify the assertions of the vendor. The tester shall consider the regulations of ISO 9564 and ISO 13491.

DTR A10 Protection Against Card Trapping

The UPT is equipped with mechanisms to prevent attacks aiming at retaining and stealing the payment card (e.g., Lebanese Loop attacks).

Guidance

Implementations may consist of shutters, detection of any obstruction in the card path, or the like.

- TA10.1** The tester shall examine the vendor's response to Section A10 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A10 of the *PCI UPT Security Requirements* for consistency relevant to A10.
- TA10.2** The tester shall visually inspect the UPT's card reader and/or the UPT in general to verify the assertions provided by the vendor in response to Section A10 PCI UPT Evaluation Vendor Questionnaire.
- TA10.3** The tester shall examine additional relevant documentation, such as functional documentation, user guidance, test documentation and assembly drawings submitted by the vendor to verify that it supports the vendor responses.
- TA10.4** The tester shall perform suitable test to verify the functionality of the mechanisms.

DTR A11 Magnetic-Stripe Reader

It is not feasible to penetrate the UPT to make any additions, substitutions, or modifications to the Magnetic-Stripe Reader or the UPT's hardware or software, in order to determine (e.g., skimming attacks must be prevented) or modify magnetic-stripe track data, without requiring an attack potential of at least 14 per UPT, for identification and initial exploitation, as defined in Appendix B.

Guidance

Countermeasures include, for instance, active detection of skimmers, active disturbance of the skimming process, or notice to the cardholder on what the reader should look like. The protection of the reader may consist of resistance of the UPT cabinet/the reader enclosure against manipulation.

Skimming attacks to recover payment card data may occur via either the attachment of external devices or attacking other areas (hardware or software) of the UPT. Both must be considered for this requirement.

Access to the inside of the UPT for routine maintenance (e.g., replenishing paper) shall not allow access to clear-text account data, e.g., by making cabling which transmits the data physically inaccessible to routine maintenance personnel or encrypting the sensitive card data transmitted internally within the UPT between components.

- TA11.1** The tester shall examine the vendor's response to Section A11 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement A11 of the *PCI UPT Security Requirements* for consistency relevant to A11.
- TA11.2** The tester shall examine additional relevant documentation, such as functional documentation, user guidance, test documentation and assembly drawings submitted by the vendor to verify that it supports the vendor responses.
- TA11.3** The tester shall visually inspect the UPT's Magnetic Stripe Reader and/or the UPT in general to verify the assertions provided by the vendor in response to Section A11 of the *PCI UPT Evaluation Vendor Questionnaire*. This will include disassembly of the test unit when necessary.
- TA11.4** The tester shall perform tests to verify that the protections of the device are such that the hardware and software of the UPT cannot be tampered without requiring an attack potential of at least 14 for identification and initial exploitation. The cost calculation shall be based on the scheme depicted in Appendix B.
The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.
- TA11.5** The tester shall develop attack scenario(s) to defeat or circumvent the protection against skimming, which require an attack potential of <14 per UPT for identification and initial exploitation. The cost calculation shall be based on the scheme depicted in Appendix B.
The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

Core Derived Test Requirements – Logical

DTR B1 Self-Test

The UPT performs a self-test, which includes integrity and authenticity tests as addressed in B4, upon start-up and at least once per day to check the firmware of the EPP and the ICC reader, the software of the UPT controller, the security mechanisms for signs of tampering, and whether the UPT is in a compromised state. In the event of a failure, the relevant component's functionality fails in a secure manner.

Guidance

Firmware is considered to be any code within the UPT that provides security protections needed to comply with these requirements. In certain instances, the test houses may request copies of source code for review of specific functions.

The device must perform an internal self-test automatically at least once every day, in addition to at power-up. It is acceptable to perform firmware integrity checks before each PIN transaction as opposed to performing them at least once every 24 hours. Self-tests after several minutes of inactivity may also be used, rather than once every 24 hours, in addition to power-up self-tests.

Software integrity tests may include SHA-1 or CRC. Authenticity testing must use cryptographic methods (MACs, digital signatures, or encryption).

The UPT controller is only in scope if it impacts one or more of the security requirements, e.g., display prompt control.

- TB1.1** The tester shall examine the vendor's response to Section B1 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B1 of the *PCI UPT Security Requirements* to verify that the UPT performs a self-test upon start-up and at least once per day to check the firmware of the EPP and the ICC reader, the software of the UPT controller, the security mechanisms for signs of tampering, and whether the UPT is in a compromised state; and that in the event of a failure, the relevant component's functionality fails in a secure manner.
- TB1.2** The tester shall examine any relevant documentation, such as the user guide or the software specification, submitted by the vendor to verify that it supports the vendor responses, including evidence of testing that confirms the relevant component fails securely in the event of self-test failure.
- TB1.3** The tester will verify that the UPT performs self-tests upon start up and on a periodic basis at least once per day to check firmware and security mechanisms for signs of tampering, and whether the UPT is in a compromised state. The tester will activate the self-test(s) and look for the result of the self-test(s) as shown by the UPT.
- TB1.4** The tester will verify that the UPT self-tests are able to detect failures and in doing so, fail in a secure manner. The vendor shall provide evidence of testing that confirms the relevant component's fails securely in the event of self-test failure.

DTR B2 Logical Anomalies

The functionality of the UPT's relevant components shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data which could result in the relevant component's outputting the clear-text PIN or other sensitive information.

Guidance

Functionality shall be considered as any functionality, via any internal or external interface, that could impact the security of the UPT's relevant components.

Vendors should provide software design rules and specifications to support answers.

The UPT controller is not in scope for this requirement.

- TB2.1** The tester shall examine the vendor's response to Section B2 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B2 of the *PCI UPT Security Requirements* to verify that the relevant component's functionality shall not be influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode and supplying wrong parameters or data that could result in the relevant component's outputting the clear-text PIN or other sensitive information.
- TB2.2** The tester shall examine any relevant documentation, such as a user guide, the specification of the relevant component's logical structure, the interface specification, the software design rules and specifications, or the software implementation submitted by the vendor to verify that it supports the vendor responses.
- TB2.3** The tester shall analyze the vendor's measures that ensure that the relevant component's functionality is not influenced by logical anomalies such as (but not limited to) unexpected command sequences, unknown commands, commands in a wrong device mode, and supplying wrong parameters or data.
- TB2.4** The tester may perform tests needed to validate the device's property. The evaluator should use his or her own judgment in determining appropriate tests. Test support shall be provided by the vendor as needed to access and use the interfaces under test.

DTR B3 Firmware Certification

The firmware, and any changes thereafter, has been inspected and reviewed using a documented process that can be audited and is certified as being free from hidden and unauthorized or undocumented functions.

Guidance

Firmware is considered to be any code within the UPT that provides security protections needed to comply with PCI requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI requirements.

- TB3.1** The tester shall examine the response to Section B3 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the firmware documentation and certification process, for consistency.
- TB3.2** The tester shall examine the support documentation submitted by the UPT vendor. The documents should be representative of a Configuration Control process that can be audited. The documentation could include firmware revision lists with updates documented, current source code check-in, checkout, and control procedures; authorized access lists, and other materials that show clear evidence that the firmware is under an auditable Configuration Control procedure.
- TB3.3** The tester shall examine details provided by the vendor that the documented process explicitly addresses how testing/auditing has been carried out to check for unauthorized and undocumented functions.
- TB3.4** The tester will verify that the device displays or otherwise makes available the revision number.

DTR B4 Firmware Updates

If the UPT allows updates of firmware or other software that impacts security, the software integrity is cryptographically authenticated by the device. If the authenticity of the update is not confirmed, the software update is rejected and deleted.

The authentication must not be performed by a component of lesser protection strength than the one for which the firmware/software is intended OR the authentication must be performed by the target component of the firmware/software.

Guidance

Firmware is considered to be any code within the UPT that provides security protections needed to comply with PCI requirements. Other code that exists within the device that does not provide security, and cannot impact security, is not considered firmware under PCI requirements.

- TB4.1** The tester shall examine the response to Section B4 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the authentication procedures for firmware updates, for consistency.
- TB4.2** The tester shall examine any additional documentation (i.e., specifications, schematics, block diagrams, etc.) that contains information that relates to firmware updates to determine if it supports the assertions made by the vendor.
- TB4.3** The tester shall verify that the UPT cryptographically authenticates the software integrity. This will be accomplished for example by performing a simulated firmware update.
- TB4.4** The tester shall verify that the UPT rejects unauthorized Firmware. This will be accomplished for example by performing a simulated firmware update with inadequate or modified authentication information.
- TB4.5** The tester shall determine by which component the authentication is performed.
- TB4.6** The tester shall determine the rank of protection strength for the component involved in firmware/software updates and that the authentication of software updates is performed by an appropriate component.
- TB4.7** The tester shall examine the vendor-supplied documentation to verify that the controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Examples of appropriate algorithms and minimum key sizes are:

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	112	1024	160	1024/160

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

AES may also be used with a key size of at least 128 bits.

Examples of acceptable hashing algorithms include SHA-1, SHA-256, SHA-384 and SHA-512. MD5 is not allowed for use.

DTR B5 Differentiation of Entered PIN

A PIN-handling component of the UPT (e.g., the EPP) never outputs information to another component (e.g., a display or a device controller), allowing the differentiation of the PIN digits entered.

Guidance

Any value can be output as long as it cannot be used to determine PIN values. Using a different value for different digit numbers or groups of numbers is not acceptable.

- TB5.1** The tester shall examine the vendor's response to Section B5 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B5 of the *PCI UPT Security Requirements* for consistency relevant to B5.
- TB5.2** The tester shall examine any relevant documentation, such as an API user guide, submitted by the vendor to verify that supports the vendor responses.
- TB5.3** The tester shall perform a test in which a PIN number is entered to verify that the UPT does not output any digits of the PIN value. The tester shall note and report any characters, signals, or tones that are outputted. The device must display the same non-significant character for all PIN-entry uses.
- TB5.4** If the UPT does not directly control the display, it must supply a suitable signal to indicate that a numeric key has been pressed and the value is stored inside the UPT. The tester shall examine the response to Section B5 of the *PCI UPT Evaluation Vendor Questionnaire* to determine the kind of signaling and to verify that the signal information is not related to the digit entered.

DTR B6 Clearing of Internal Buffers

Sensitive information shall not be present any longer or used more often than strictly necessary. Online PINs are encrypted within the EPP immediately after PIN entry is complete and has been signified as such by the cardholder, e.g., via pressing the enter button.

The UPT must automatically clear its internal buffers when either:

- **The transaction is completed, or**
- **The UPT has timed out waiting for the response from the cardholder or merchant.**

Guidance

Vendor shall provide documentation of test results for inspections of internal buffers.

Plain-text PINs must not exist for more than one minute maximum from the completion of the cardholder's PIN entry. In all cases, erasure of the plain-text PIN must occur before the tamper-detection mechanisms can be disabled using attack methods described in A1.1.

The UPT may support the encipherment of the PIN multiple times as part of a transaction series; however, the PIN shall only be enciphered using the same PIN encipherment key and transaction data, and not different keys or transaction data.

TB6.1 The tester shall examine the vendor's response to Section B6 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B6 of the *PCI UPT Security Requirements* to verify:

- That sensitive information shall not be present any longer or used more often than strictly necessary;
- The immediate encryption of online PIN data; and
- That the UPT automatically clears its internal buffers when either the transaction is completed or the UPT has timed out waiting for the response from the cardholder or merchant. The vendor must specify the states "completion of transaction" and "timeout" and define the appropriate actions.

TB6.2 The tester shall examine any relevant documentation, including vendor test results for inspections of internal buffers, the user guide, the software specification, or the software implementation submitted by the vendor to verify that it supports the vendor responses.

TB6.3 The tester will verify that the vendor has identified all data that is automatically cleared when the transaction is completed and that all sensitive data is included. Passwords, plain-text cryptographic keys, or key components outside of the crypto-processor, and PIN values are considered sensitive data.

TB6.4 The tester will verify that all data is automatically cleared when either the transaction is completed or the UPT has timed out waiting for the response from the cardholder or merchant. The tester will determine the appropriate test actions to be taken. For instance, by performing a partial simulated transaction to verify the behavior at timeout, or in general by entering the states that have been defined by the vendor under TB6.1.

DTR B7 Protection of Sensitive Services

Access to sensitive services requires authentication. Sensitive services provide access to the underlying sensitive functions. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs and passwords. Entering or exiting sensitive services shall not reveal or otherwise affect sensitive information.

Guidance

Authentication shall be considered as dual control techniques when entering sensitive information through a secure user interface, or cryptographic techniques when entering electronic data. The use of other techniques to access sensitive services results in the device being unable to use previously existing keying material.

A sensitive service (state) allows the execution of functions that are not available during normal use—e.g., load a master key, delete stored transactions, alter device configuration, etc.

Key components entered manually constitute sensitive data during entry and the device shall not differentiate via sound or display the entry of different values.

- TB7.1** The tester shall examine the vendor's response to Section B7 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B7 of the *PCI UPT Security Requirements* for consistency relevant to B7.
- TB7.2** The tester shall examine any relevant documentation (such as an API user guide) submitted by the vendor to verify that it supports the vendor assertions with regard to the control of sensitive services.
- TB7.3** The tester shall verify from vendor documentation that the vendor has identified all sensitive services, data and secure modes. Sensitive functions are those functions that process sensitive data such as cryptographic keys, PINs, and passwords. The tester shall verify from vendor documentation that sensitive services are entered, used, and exited securely and that mode transitions (e.g., from operational to maintenance) do not reveal or otherwise affect sensitive information.
- TB7.4** The tester shall verify from vendor documentation and from functional testing that sensitive services require authentication.
- TB7.5** The tester shall verify from vendor documentation and from functional testing that entering and exiting sensitive services does not reveal or otherwise affect sensitive information.
- TB7.6** The tester shall verify from vendor documentation that sensitive services are entered, used, and exited securely and that mode transitions (e.g., from operational to maintenance) do not reveal or otherwise affect sensitive information.

TB7.7 If access to sensitive services requires input by the keypad, the tester shall verify that the protections for PIN data, such as the following, are also afforded to data entered while accessing sensitive services:

- Data inputs cannot be discerned from any displayed characters.
- Data inputs cannot be discerned by monitoring audible or electro-magnetic emissions.
- Sensitive data is cleared from internal buffers upon exiting the sensitive mode.

The testing shall include:

- Entering data while accessing sensitive services.
- Document review.

TB7.8 If mode transitions require input by a separate interface device, such as a key loader, the tester will document the mechanism(s) and methodology used.

DTR B8 Sensitive Services Limits

To minimize the risks from unauthorized use of sensitive services, limits on the number of actions that can be performed and a time limit shall be imposed, after which the UPT is forced to return to its normal mode.

Guidance

This applies to each and any transition to the use of sensitive services.

- TB8.1** The tester shall examine the vendor's response to Section B8 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B8 of the *PCI UPT Security Requirements* for consistency relevant to B8.
- TB8.2** The tester shall examine any relevant documentation, such as the user guide or the software specification, submitted by the vendor to verify that it supports the vendor responses.
- TB8.3** The tester shall examine the rationale provided by the vendor in Section B8 of the *PCI UPT Evaluation Vendor Questionnaire* to verify the following:
 - The vendor has provided a rationale for the value chosen as a limit on the number of actions and the time limits imposed.
 - The vendor has provided a rationale as to how the limits minimize the risks from unauthorized use of sensitive services.
- TB8.4** The tester shall verify the limits placed on the number of actions by causing the UPT to access sensitive services and attempting to exceed the limit. Once the limit is exceeded the tester will verify that the UPT has returned to its normal mode.
- TB8.5** The tester shall verify that a time limit is imposed such that after one minute of inactivity while accessing sensitive services, the UPT returns to its normal state. This will be accomplished by attempting to use sensitive functions after the time limit has been exceeded.
- TB8.6** The tester shall verify that a time limit is imposed such that fifteen (15) minutes after accessing sensitive services, the UPT returns to its normal mode. This will be accomplished by attempting to use sensitive functions after the time limit has been exceeded. To prevent the UPT from reaching a limit of inactivity, sensitive functions will be used throughout the fifteen minutes.

DTR B9 Random Numbers

If the UPT generates random numbers in connection with security over sensitive data, the random-number generator has been assessed to ensure it is generating numbers sufficiently unpredictable.

- TB9.1** The tester shall examine the vendor's response to Section B9 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B9 of the *PCI UPT Security Requirements* for consistency relevant to B9.
- TB9.2** The tester shall compare the vendor-supplied documentation, such as the specification of the random number generator and test documentation, submitted by the vendor to verify that it supports vendor responses.
- TB9.3** The tester shall verify test information provided by the vendor to assess whether the random numbers are sufficiently unpredictable. The tester shall use a suitable test method (for example, those listed in NIST PUB 800-22). See Appendix C.

DTR B10 Exhaustive PIN Determination

The EPP has characteristics that prevent or significantly deter the use of a stolen device for exhaustive PIN determination.

Guidance

The following are examples of techniques that may be used to prevent an exhaustive PIN determination attack, such as one using electromechanical solenoids to depress the keys so as to try all possible PINs until the ciphertext produced equals the ciphertext recorded when the UPT was in operational use:

- *Use of a unique key per transaction technique. (Prevents the attack.)*
- *Preventing the entry of the PIN through other than the keypad, and limiting the rate at which the UPT will encrypt PINs to the average (for example, over 120 transactions) of one per 30 seconds. (Deters the attack.)*
- *The device is exclusively used for offline PIN and the ICC reader is integrated into the EPP.*

Offline devices that do not have the EPP and the ICC reader integrated into the same secure module, and which are using ISO format 0 and are not using a unique key per transaction for the conveyance of the PIN from the point of entry to the ICC reader, must comply with this requirement.

- TB10.1** The tester shall examine the response to Section B10 of the *PCI UPT Evaluation Vendor Questionnaire* relating to characteristics that prevent or significantly deter the use of a stolen device for exhaustive PIN determination.
- TB10.2** The tester shall examine any additional documentation (i.e., specifications, schematics, block diagrams, etc.) that contains information that relates to characteristics that prevent or significantly deter exhaustive PIN determination to determine if it supports the assertions made by the vendor.
- TB10.3** The tester shall perform functional testing to verify the UPT characteristics regarding B10.

DTR B11 Key Management

The key-management techniques implemented in the UPT conform to ISO 11568 and/or ANSI X9.24. Key-management techniques must support ANSI TR-31 or an equivalent methodology for maintaining the TDEA key bundle.

Note: Clear keys or clear-key parts must not be loaded using the service module.

Guidance

TDES key components shall be combined via either XOR'ing of full-length key components or via implementation of a recognized secret sharing scheme, e.g., Shamir. Private key components shall be combined using a recognized secret sharing scheme.

A UPT may include more than one compliant key exchange and storage scheme.

This does not imply that the device must enforce TR-31 or an equivalent scheme, but it must be capable of implementing such a scheme as a configuration option.

For all TDEA modes of operation, the three cryptographic keys (K1, K2, K3) define a TDEA key bundle (see X9.52). The bundle and the individual keys must:

- *Be secret;*
- *Be generated randomly or pseudo-randomly;*
- *Have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized source;*
- *Be used in the appropriate order as specified by the particular mode;*
- *Be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged; and*
- *Cannot be unbundled for any purpose.*

Documentation must be provided demonstrating how the methodology meets these criteria.

- TB11.1** The tester shall examine the response to Section B11 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the method of key management in use in the UPT, for consistency.
- TB11.2** The tester shall examine any relevant documentation such as a user guide or the API Programmer's guide, submitted by the vendor to verify that it supports vendor responses.
- TB11.3** The tester shall determine from vendor documentation the key-management technique used for firmware and application updates. Symmetric key techniques must include the use of Unique Key(s) per Device.
- TB11.4** The tester shall examine any additional documentation (e.g., API reference, design documentation, key management specification) that describes the implemented key exchange and storage techniques to determine if it supports the assertions made by the vendor.

TB11.5 The tester shall verify that the loading of private and secret keys uses one or more of the following methods:

- a) When entering plain-text secret keys through the keypad, they must be entered as two or more components and require the use of at least two passwords/PINs. The passwords must be entered through the keypad or else conveyed encrypted into the device. These passwords/PINs must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Passwords/PINs that are unique per device can be made optionally changeable by the acquirer, but this is not required. Passwords/PINs are at least five characters.

Entry of key components without the use of at least two separate passwords/PINs results in the zeroization of pre-existing secret keys, i.e., the invoking of the key loading function/command causes the zeroization prior to the actual loading of the new key. For devices supporting multiple key hierarchies (e.g., multi-acquirer devices), only the hierarchy (specific TMK and working keys) associated with the key being loaded must be zeroized.

- b) For injecting plain-text secret or private keys from a key loader (which has to be some type of secure cryptographic device), either the key loader or the UPT or both must require two or more PINs/passwords before injecting the plain-text key into the UPT. (*Note: This may be the entire key—if components, each component requires a separate password.*) Passwords/PINs are at least five characters. These passwords are entered directly through the keypad of the applicable device or are conveyed encrypted into the device. These passwords/PINs must either be unique per device (and per custodian), except by chance, or if vendor default, they are pre-expired and force a change upon initial use. Plain-text keys or their components are never permitted over a network connection.

Injection of plain-text secret keys or their components where the UPT does not itself require the use of at least two PINs/passwords for injection results in the zeroization of pre-existing secret keys. For devices supporting multiple key hierarchies (e.g., multi-acquirer devices), only the hierarchy (specific TMK and working keys) associated with the key being loaded must be zeroized.

- c) For encrypted values injected into the UPT, either from a key loader or from a network host, or via loading through the keypad, the ability of the UPT to successfully decrypt the value and use it is sufficient. In this case, the loading of the key encipherment key would have been done under dual control, e.g., in examples a) and b) above.
- d) Remote key loading techniques using public key methods requires compliance with PCI defined criteria for key sizes and mutual authentication between host and UPT. For UPTs generating their own key values, the generation process must meet the criteria defined in the random number appendix of the DTRs and validation that appropriate key sizes are used. The protocol must meet the criteria stipulated in Annex A of the *PCI PIN Security Requirements*.

TB11.6 The vendor may alternately provide user documentation detailing the management of cryptographic keys following the principles of dual control and split knowledge and implementing the use of a secure cryptographic device for management of these keys. That is, the process exists upstream of the UPT.

TB11.7 If a public key technique for the distribution of symmetric secret keys is used, it must:

- Use public and private key lengths that are deemed acceptable for the algorithm in question (e.g., 1024-bits minimum for RSA, see also DTR A7.3).
- Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question.
- Provide for mutual device authentication for both the host and the UPT, including assurance to the host that the UPT actually has (or actually can) compute the session key and that no other entity other than the UPT specifically identified can possibly compute the session key.

The following are the minimum key sizes and parameters for the algorithm(s) in question that must be used for key transport, exchange or establishment:

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	112	1024	160	1024/160

DES refers to TDES keys with non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

AES may also be used with a key size of at least 128 bits.

For Diffie-Hellman implementations:

- Entities must securely generate and distribute the system-wide parameters: generator g , prime number p and parameter q , the large prime factor of $(p - 1)$. As described in ANSI X9.42, parameter p must be at least 1024 bits long, and parameter q must be at least 160 bits long. Each entity generates a private key x and a public key y using the domain parameters (p, q, g) . Each private key shall be statistically unique, unpredictable, and created using an approved random number generator as described in this document.
- Entities must authenticate the Diffie-Hellman public keys using either DSA, a certificate, or a symmetric MAC (based on TDES—see ISO 16609 – *Banking – Requirements for message authentication using symmetric techniques*; Method 3 should be used).

TB11.8 The tester shall determine from vendor documentation the cryptographic keys present or ever used by the device and list the details in a key summary table. An example of key types in such a table is:

Key Name	Purpose/Usage	Algorithm	Size (Bits)	Generated By:	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)	Unique per device/acquirer/vendor-specific/other (describe)
Terminal Master Key (TMK)	Encryption of working keys (PEK, MAC) for down-line transmission to the device	TDES	128	Acquirer	2 or 3 plain-text components	One	Device
MAC Key	Message authentication	TDES, DES	128 or 64	Acquirer	Enciphered under the TMK	Two	Device
PIN-encryption Key (PEK)	PIN encipherment for online PIN	TDES, DES	128 or 64	Acquirer	Enciphered under the TMK	Two	Device
Fixed Key	PIN encipherment for online	TDES, DES	128 or 64	Acquirer	2 or 3 plain-text components	One	Device
IPEK	Initial DUKPT Key	TDES	128	Acquirer	Plain-text from Key Injection Device	One	Device
DUKPT PEKs (Future Keys Register)	PIN encipherment for online PIN	TDES	128	Acquirer	Derived originally from IPEK	Up to 21 Future Keys	Device
KPT	PIN encipherment between EPP and IC card reader	TDES	128	Acquirer	2 or 3 plain-text components	One	Device
Payment Scheme (Certification Authority) Public Keys	Authentication of issuer key from IC card.	RSA	Varies	Payment Schemes	EMV Public Key Certificate	Six per payment schemes – three payment schemes	Payment scheme-specific
Manufacturer Firmware Authentication Root or Sub-CA Public Key	Authentication of firmware updates as part of a certificate chain to the manufacturer root key	RSA	2048	Manufacturer	Certificate signed with manufacturer's private key	One	Vendor-specific
Manufacturer Authentication Root or Sub-CA Public Key	Authentication of acquirer-signed applications as part of a certificate chain to the manufacturer root key	RSA	2048	Manufacturer	Certificate signed with manufacturer's private key	One	Vendor-specific
Acquirers Application Public Authentication Key	Authentication of acquirer-signed applications as part of certificate chain to manufacturer root key	RSA	2048	Acquirer	Public Key Certificate signed by manufacturer root or sub-CA private key	One	Acquirer
Manufacturer Authentication Root or Sub-CA Private Key	Signing firmware updates or the acquirer application signing public key	RSA	2048	Manufacturer	Managed at manufacturer's secure facility under dual control	One	Vendor-specific
Acquirer's Application Private Authentication Key	Signing application updates	RSA	2048	Acquirer	Managed at acquirer's secure facility under dual control	One	Acquirer

- TB11.9** The tester shall determine from vendor documentation all storage and usage locations for each key e.g., ROM, external RAM, EPROM, processor chip, etc., and list the details in a key summary table.
- TB11.10** The tester shall determine from vendor documentation how (e.g., active or passive erasure) each key is destroyed for all device states (power-on, power-off, sleep mode) and list the details in a key summary table.

DTR B12 Encryption Algorithm Test

The PIN-encryption technique implemented in the UPT is a technique included in ISO 9564.

TB12.1 The tester shall examine the response to Section B12 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the TDES PIN-encryption implementation in the UPT, for consistency and compliance with ISO 9564.

TB12.2 The tester shall examine any additional documentation (i.e., specifications, schematics, block diagrams, etc.) that contains information that relates to the PIN-encryption technique implemented in the UPT.

Note: The UPT must support at least one of the following key-management techniques using TDES as described in ANSI X9.24 and ANSI X9.52:

- DUKPT
- Fixed
- Master/Session

The UPT must also support at least one of the following PIN Block Formats if supporting online PIN Entry:

- ISO Format 0
- ISO Format 1
- ISO Format 3

For offline PIN:

- a) The PIN that is submitted by the IC reader to the IC shall be contained in a PIN block conforming to ISO Format 2 PIN block. This applies whether the PIN is submitted in plain text or enciphered using an encipherment key of the IC.
- b) Where the ICC reader is not integrated into the EPP, and PINs are enciphered only for transmission between the PIN entry device and the IC reader, the UPT shall use one of the PIN block formats specified in ISO 9564-1. Where ISO Format 2 PIN blocks are used, a unique key per transaction method in accordance with ISO 11568 shall be used. Format 2 shall be used only in connection with either offline PIN verification or PIN-change operations in connection with ICC environments.

TB12.3 The tester shall perform a transaction with a known encryption key. The tester shall use this key to create an encrypted PIN block with a test system, using the Primary Account Number, and PIN with the format (the format must be either ISO format 0, 1 or 3, specified by the vendor. The corresponding encrypted PIN block shall be generated by the UPT with a simulated transaction. If both encrypted PIN blocks are identical, the UPT is using the TDES algorithm and the specified format for encryption.

DTR B13 Encryption or Decryption of Arbitrary Data Within the Device

It is not possible to encrypt or decrypt any arbitrary data using any PIN-encrypting key or key-encrypting key contained in the UPT. The UPT must enforce that data keys, key-encipherment keys, and PIN-encryption keys have different values.

Guidance

PIN-encryption keys shall only be used to encrypt PIN data. Key-encrypting keys shall only be used to encrypt keys. PIN keys shall never be used to encrypt keys. Key-encrypting keys shall never be used to encrypt PIN data.

The intent of the requirement is to help ensure that these keys are not intentionally used for multiple purposes. Thus the integrity check applies when the device is initially loaded with these keys. Session keys (working keys such as PIN, data, and MAC keys) or key-encipherment keys subsequently downloaded during normal operations must be randomly generated, and there should only be collisions (duplication) by chance.

This is not intended to require that the device compare keys across different key hierarchies associated with different acquirers.

- TB13.1** The tester shall examine the response to Section B13 of the *PCI UPT Evaluation Vendor Questionnaire* relating to encryption and decryption of arbitrary data, for consistency.
- TB13.2** The tester shall examine any additional documentation such as the API Programmer's guide, submitted by the vendor to verify that it supports vendor responses.
- TB13.3** The tester shall verify the following:
 - a) PIN-encryption keys are only used to encrypt PIN data.
 - b) Key-encrypting keys are only used to encrypt keys.
 - c) PIN keys shall never be used to encrypt keys.
 - d) Key-encrypting keys shall never be used to encrypt PIN data.
- TB13.3** The tester shall verify by testing that the UPT enforces that data keys, key-encipherment keys, and PIN-encryption keys have different values, e.g., by attempting to load keys of different types with effectively the same value.

DTR B14 Clear-Text Key Security

There is no mechanism in the UPT that would allow the outputting of a private or secret clear-text key or clear-text PIN, the encryption of a key or PIN under a key that might itself be disclosed, or the transfer of a clear-text key from a component of high security into a component of lesser security.

Guidance

Clear-text secret and private keys and clear-text PINs must not exist in unprotected environments.

- TB14.1** The tester shall examine the response to Section B14 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the output of clear-text keys and protection of PINs for consistency. The clear-text PIN must never exist in an unprotected environment.
- TB14.2** The tester shall examine the response to Section B14 of the *PCI UPT Evaluation Vendor Questionnaire* relating to encryption of a key or PIN under a key that might itself be disclosed, for consistency.
- TB14.3** The tester shall examine the response to Section B14 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the transfer of a key from a high-security component to a lower-security component, for consistency.
- TB14.4** The tester shall examine any additional documentation (i.e., API Programmer's guide, specifications, block diagrams, etc.) that contains information that relates to any of the aforementioned to determine if it supports the assertions made by the vendor.

DTR B15.1

Prompts Under Control of the Cryptographic Unit

All prompts for non-PIN data entry are under the control of the cryptographic unit of the UPT and circumventing the control requires an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B. Prompts cannot feasibly be altered without causing the erasure of the unit's cryptographic keys. If the prompts are stored outside the cryptographic unit, cryptographic mechanisms must exist to ensure the authenticity and the proper use of the prompts and that modification of the prompts or improper use of the prompts are prevented.

Guidance

B15.1 should be complied with for devices that allow prompts to be changed as part of firmware updates. B15.2 should be selected when the prompts are fixed and cannot be updated; for example, when they are stored in ROM. B15.3 is appropriate for all other devices where non-PIN data can be entered by the cardholder.

Non-PIN data refers to numeric data other than the PIN that is entered via the keypad.

Cryptographic keys that are never used to encrypt or decrypt data; or are not used for authentication, do not need to be considered secret data, and therefore do not need to be erased.

TB15.1.1 The tester shall examine the response to Section B15.1 of the *PCI UPT Evaluation Vendor Questionnaire*, relating to user prompts, and alteration of prompts for consistency. The tester shall verify that mechanisms exist to ensure the authenticity and proper use of the prompts and modification of the prompts or improper use of the prompts is prevented.

TB15.1.2 The Tester shall examine all possible prompts to determine if any can be used in conjunction with numeric entry in the clear.

TB15.1.3 The tester shall examine any additional documentation (i.e., specifications, schematics, block diagrams, etc.) that contains information on non-PIN data entry and prompts for non-PIN data entry, and on data entry and erasure, and on how authentic user prompts are generated and administered to determine if it supports the assertions made by the vendor.

TB15.1.4 The tester shall examine the vendor-supplied documentation to verify that the controls to ensure the authenticity and the proper use of the prompts provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Examples of appropriate algorithms and minimum key sizes are:

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	112	1024	160	1024/160

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

AES may also be used with a key size of at least 128 bits.

Examples of acceptable hashing algorithms include SHA-1, SHA-256, SHA-384 and SHA-512. MD5 is not allowed for use.

TB15.1.5 The tester shall develop attack scenarios to circumvent the control of the display by the UPT, which require an attack potential of <16 per UPT for identification and initial exploitation as defined in Appendix B to circumvent.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR B15.2 Altering User Interface Prompts Cost Analysis

The unauthorized alteration of prompts for non-PIN data entry into the PIN entry keypad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted, cannot occur without requiring an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B.

Guidance

B15.1 should be complied with for devices that allow prompts to be changed as part of firmware updates. B15.2 should be selected when the prompts are fixed and cannot be updated; for example, when they are stored in ROM. B15.3 is appropriate for all other where non-PIN data can be entered by the cardholder.

Non-PIN data refers to numeric data other than the PIN that is entered via the keypad.

- TB15.2.1** The tester shall examine the assertions provided by the vendor in response to Section B15.2 of the *PCI UPT Evaluation Vendor Questionnaire* relating to unauthorized alterations of prompts.
- TB15.2.2** The tester shall examine any additional documentation (i.e., specifications, schematics, block diagrams, etc.) that contains information on how prompts are generated and administered to determine if it is possible to perform unauthorized alterations of prompts.
- TB15.2.3** The tester shall develop attack scenarios for the unauthorized alteration of prompts for non-PIN data entry into the PIN entry key pad such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted. The attack potential calculation shall be based on the scheme depicted in Appendix B. If an attack scenario can be developed that requires an attack potential of less than 16 per UPT for identification and initial exploitation as defined in Appendix B, the vendor assertion cannot be verified.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR B15.3 User Interface Consistency

The UPT (application) must enforce the correspondence between the display messages visible to the cardholder and the operating state (i.e., secure or non-secure mode) of the EPP—e.g., by using cryptographic authentication.

If commands impacting the correspondence between the display messages and the operating state of the EPP are received from an external device (e.g., a store controller), the commands enabling data entry must be authenticated.

The alteration of the correspondence between the display messages visible to the cardholder and the operating state of the EPP cannot occur without requiring an attack potential of at least 16 per UPT for identification and initial exploitation as defined in Appendix B of the PCI UPT DTRs,

Guidance

B15.1 should be complied with for devices that allow prompts to be changed as part of firmware updates. B15.2 should be selected when the prompts are fixed and cannot be updated; for example, when they are stored in ROM. B15.3 is appropriate for all other where non-PIN data can be entered by the cardholder.

Non-PIN data refers to numeric data other than the PIN that is entered via the keypad.

The ability to physically access the connection between the EPP, UPT controller, and ICC reader must not facilitate attacks to interfere with that correspondence and especially to collect clear PIN data (e.g., commands are authenticated and/or enciphered). Keys used for such protocols must only be used for this purpose, and may then be stored and used in the UC in the clear. It is not required to use a cryptographic module in the UC for that purpose.

TB15.3.1 The tester shall examine the assertions provided by the vendor in response to Section B15.3 of the *PCI UPT Evaluation Vendor Questionnaire* relating to the control of the EPP operating modes and the corresponding display messages visible to the cardholder, for consistency.

TB15.3.2 The tester shall examine any additional documentation (i.e., API Programmer's guide, specifications, schematics, block diagrams, etc.) that contains information that relates to the control of the EPP operating modes and the corresponding display messages visible to the cardholder, to determine if it supports the assertions made by the vendor.

TB15.3.3 The tester shall verify by testing, that the ability to physically access the connection between the EPP, UPT controller and ICC reader must not facilitate attacks to interfere with that correspondence. If commands are authenticated and/or enciphered, the existence and efficiency of this mechanism has to be verified.

TB15.3.4 The tester shall examine the vendor-supplied documentation to verify that the controls provide for unique accountability and utilize key sizes appropriate for the algorithm(s) in question. Examples of appropriate algorithms and minimum key sizes are:

Algorithm	DES	RSA	Elliptic Curve	DSA
Minimum key size in number of bits	112	1024	160	1024/160

DES refers to non-parity bits. The RSA key size refers to the size of the modulus. The Elliptic Curve key size refers to the minimum order of the base point on the elliptic curve; this order should be slightly smaller than the field size. The DSA key sizes refer to the size of the modulus and the minimum size of a large subgroup.

AES may also be used with a key size of at least 128 bits.

Examples of acceptable hashing algorithms include SHA-1 and SHA-256. MD5 is not allowed for use.

TB15.3.5 If commands impacting the correspondence between the display messages and the operating state of the EPP are received from an external device (e.g., a store controller), the tester has to verify, that the commands enabling data entry are authenticated, and that the mechanisms are efficient.

TB15.3.6 The tester shall develop attack scenarios for the alteration of the correspondence between the display messages visible to the cardholder and the operating state of the EPP such that PINs are compromised, i.e., by prompting for the PIN entry when the output is not encrypted. The attack potential calculation shall be based on the scheme depicted in Appendix B. If an attack scenario can be developed that requires an attack potential of less than 16 per UPT for identification and initial exploitation as defined in Appendix B, the vendor assertion cannot be verified.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR B16 Application Separation

If the UPT supports multiple applications, it must enforce the separation between applications with security impact from those without security impacts. It must not be possible that one application interferes with or tampers another application or the OS of the UPT, including modifying data objects belonging to another application.

Guidance

Applications are considered to be separated by access rights. OS is considered all code, which is responsible to enforce, manage, or change such access rights. Therefore, OS code is necessarily part of the firmware as defined with B1.

Vendors should provide configuration lists and description of the separation mechanism to support answers.

- TB16.1** The tester shall examine the vendor's response to Section B16 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B16 of the *PCI UPT Security Requirements* to verify that if the UPT supports multiple applications, it enforces the separation between applications with security impact from those without security impacts. Furthermore, the tester shall examine which part of the firmware is considered OS, and which part is considered as application with security impact.
- TB16.2** The tester shall examine any relevant documentation, such as the user guide, specification of the UPT's logical structure, configuration lists, description of separation mechanisms, interface specifications, or the software implementation submitted by the vendor to verify that it supports the vendor responses.
- TB16.3** The tester shall analyze the vendor's measures that ensure that the UPT enforces the separation between applications with security impact from those without security impacts. The tester will verify that it is not possible that one application interferes with or tampers another application or the OS of the UPT, especially to access, use or modify data objects belonging to another application, even if they are distributed over separate components of the UPT.
- TB16.4** If the OS and / or any application with security impact are distributed over separate components of the UPT, the tester will verify that the communication in between separated parts is consistent with the separation mechanisms as described by the vendor. The vendor shall provide evidence concerning the communication in between the separated parts and how the communication protocols maintain the separation of applications with security impact from those without security impacts.

DTR B17 Minimal Configuration

The operating system of the UPT must contain only the components and the services necessary for the intended operation. It must be configured for least privilege.

Guidance

The intended operation is considered as the functionality relevant to B2. For multi-application UPT the intended operation furthermore includes the operation of applications without security impacts.

OS modules such as, for example, peripheral drivers, file systems, or inter-process communication protocols shall be regarded as components. Applications responding to external interfaces or communicating with the firmware shall be regarded as services.

Vendors should provide configuration lists and software specifications to support answers.

- TB17.1** The tester shall examine the vendor's response to Section B17 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B17 of the *PCI UPT Security Requirements* to verify that the operating system and the related software of the UPT contain only the components and the services necessary for the intended operation.
- TB17.2** The tester shall examine any relevant documentation, such as a user guide, the specification of the UPT's logical structure, the UPT interface specification, or the software implementation submitted by the vendor to verify that it supports the vendor responses.
- TB17.3** The tester shall verify that all components and services indicated in the configuration list are necessary for the intended operation. For that purpose, the vendor shall provide a configuration list, which shows all OS components and other software with an explanation of the purpose and a rationale for its presence.
- TB17.4** The tester shall verify that the operating system is enforcing least privilege.
- TB17.5** The tester will examine the methods and tools provided by the vendor, which ensure, that the intended software configuration of the UPT is maintained and that updates and release changes do not affect the secure configuration of the O/S.

DTR B18 Control of any Numeric Interface

The UPT must be equipped with only one payment card PIN-acceptance interface—e.g., a keyboard. If another interface is present that can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry—e.g., it must not have numeric keys, or it is not possible to use it otherwise for numeric entry or it is controlled in a manner consistent with B15.

Guidance

A keyboard may be a touch screen if the cardholder can input numeric data to it.

Any interface of the UPT that can be used to accept numeric entry must be controlled.

- TB18.1** The tester shall examine the vendor's response to Section B18 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement B18 of the *PCI UPT Security Requirements* to verify that any interface of the UPT that can be used to accept payment card numeric entry is controlled, and that the UPT is equipped with only one PIN-accepting keyboard.
- TB18.2** The tester shall examine any additional documentation (i.e., user guide, specifications, block diagrams, etc.) that contains information about data entry devices and its possible use for numeric entry, submitted by the vendor to verify that it supports the vendor assertions.
- TB18.3** The tester shall visually inspect the UPT to verify the assertions provided by the vendor in the *PCI UPT Evaluation Vendor Questionnaire* in order to verify that:
 - The UPT must be equipped with only one payment card PIN-accepting keyboard, and
 - If another interface is present which can be used as a keyboard, a mechanism must exist to prevent its use for PIN entry, e.g. it must not have numeric keys, or it must not be possible to use it otherwise for numeric entry or it is controlled in a manner consistent with B15.
- TB18.4** If the UPT is equipped with more than one keyboard, and if the keyboard not intended for payment card PIN entry may be operated to accept numeric entry (e.g. since it is equipped with numeric keys or since it is fully programmable, like a touch screen), the tester shall verify that these numeric modes may not be used to enter a payment card PIN, especially that a possible use of numeric entry modes does not interfere with Requirement B15.

Online Derived Test Requirements

DTR C1 Key Substitution

If the UPT can hold multiple PIN encryption keys and the key to be used to encrypt the PIN can be externally selected, then the UPT prohibits unauthorized key replacement and key misuse.

Guidance

The term “externally selected” means selected by an interface function to the UPT component that performs the PIN encryption. Both human interfaces and command interfaces are considered, and both direct and indirect.

External selection also includes interference with or manipulation of the data by which the PIN-encrypting UPT component selects the key to be used.

Keys may be selected through the UPT keypad, or commands sent from another device such as an electronic cash register. Any commands sent from another device must be cryptographically authenticated to protect against man-in-the-middle and replay attacks.

C1 is not applicable to devices that do not include commands for external key selection, or cannot hold multiple key hierarchies related to PIN encryption.

If an application can select keys from multiple key hierarchies, the UPT must enforce authentication of commands used for external key selection. If the UPT only allows an application to select keys from a single hierarchy, then command authentication is not required.

- TC1.1** The tester shall examine the response to Section C1 of the *PCI UPT Evaluation Vendor Questionnaire* relating to multiple keys and unauthorized key replacement and key misuse, for consistency.
- TC1.2** The tester shall examine any additional documentation such as a user’s manual or the API Programmer’s guide submitted by the vendor to verify that it supports vendor responses.

Offline Derived Test Requirements

DTR D1 Penetration Protection

It is not feasible to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, without requiring an attack potential of at least 16 for identification and initial exploitation, as defined in Appendix B.

- TD1.1** The tester shall examine the vendor's response to Section D1 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D1 of the *PCI UPT Security Requirements* for consistency relevant to D1.
- TD1.2** The tester shall examine any relevant documentation, such as assembly drawings, submitted by the vendor to verify that it supports the vendor responses.
- TD1.3** The tester shall examine the device to verify that the asserted protections exist and conform to the descriptions provided by the vendor in documentation. This will include disassembly of the test unit when necessary.
- TD1.4** The tester shall develop attack scenarios to penetrate the ICC reader to make any additions, substitutions, or modifications to either the ICC reader's hardware or software, in order to determine or modify any sensitive data, with an attack potential of < 16. The attack potential calculation shall be based on the scheme depicted in Appendix B.

The tester may perform any test needed to validate the attack scenario. The tester will use his or her own judgment in determining the appropriate tests and whether the attack will be performed in its entirety or in part to verify the theory.

DTR D2.1 ICC Reader Slot Geometry

The slot of the ICC reader into which the ICC is inserted does not have sufficient space to hold a PIN-disclosing “bug” when a card is inserted. The slot of the IC card reader into which the IC card is inserted cannot feasibly be enlarged to provide space for a PIN-disclosing bug. It is not possible for both an IC card and any other foreign object to reside within the card-insertion slot.

Guidance

The attack potential of the evaluation shall be commensurate with that of A1, i.e., the attack potential shall not be less than 25.

The objective of D2 is to guard against a PIN-disclosing bug being inserted into the UPT through the card slot. The volume of space accessible via the card slot that could be utilized by an attacker can vary with the geometry of the space and attack methods. For this reason, the requirement does not prohibit a specific volume. Rather, the feasibility of effective bug placement is to be considered when assessing D2 compliance. Examples of these considerations are:

- *Contact points must be present for the bug to connect to;*
- *The bug and wires must not obstruct normal operation;*
- *The placement of the bug must not cause tamper evidence that would be noticed by a typical cardholder.*

D2 is written with the understanding that the opening (slot) is a potential point of attack for the insertion of a tapping mechanism. Space accessible via the IC card slot large enough to conceal a PIN-disclosing bug is not allowed. There must not be space accessible via the card slot large enough to conceal an IC card chip and small battery.

TD2.1.1 The tester shall examine the vendor's response to Section D2.1 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D2.1 of the *PCI UPT Security Requirements* for consistency relevant to D2.1.

TD2.1.2 The tester shall examine any relevant documentation (such as assembly drawings) submitted by the vendor to verify that it supports the vendor responses.

TD2.1.3 The tester shall examine the ICC reader slot to verify that:

- The slot does not have sufficient space to hold a PIN-disclosing bug when a card is inserted.
- The slot cannot feasibly be enlarged to provide space for a PIN-disclosing bug. The tester will develop attack scenarios where necessary.
- It is not possible for both an IC card and any other foreign object to reside within the card-insertion slot. For instance, it will be verified that the slot is not large enough to hold more than one card.

This will include disassembly of the test unit when necessary. Measurements of spaces within the slot will be made when relevant.

TD2.1.4 The tester shall develop an attack scenario to enlarge the slot. The tester will use his or her experience to determine what type of testing is necessary to determine the attack feasibility.

TD2.1.5 The tester shall perform a simulated transaction whilst inserting two cards into the slot. If it is possible to insert two cards and perform the transaction, then the device does not comply with this requirement.

DTR D2.2 ICC Reader Slot Visibility

The opening for the insertion of the IC card is in full view of the cardholder prior to card insertion so that any untoward obstructions or suspicious objects at the opening are detectable.

- TD2.2.1** The tester shall examine the vendor's response to Section D2.2 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D2.2 of the *PCI UPT Security Requirements* for consistency relevant to D2.2.
- TD2.2.2** The tester shall examine a test unit to verify vendor assertions that the ICC reader's slot is in full view of the cardholder so that any untoward obstructions or suspicious objects at the opening are detectable. The construction of the device should be such that the entire slot opening is in full view of the cardholder prior to card insertion.

DTR D3 ICC Reader Construction (Wires)

The ICC reader of the UPT is constructed and integrated into the UPT so that wires running out of the slot of the ICC reader to a recorder or a transmitter (an external bug) can be observed by the cardholder.

- TD3.1** The tester shall examine the vendor's response to Section D3 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D3 of the *PCI UPT Security Requirements* for consistency relevant to D3.
- TD3.2** The tester shall examine a test unit to verify vendor assertions that the ICC reader is constructed so that wires running out of the slot can be observed by the cardholder. The reader enclosure shall not have any seams or channels around the slot that would allow the concealment of wires.

DTR D4 PIN Protection During Transmission Between UPT and ICC Reader

- D4.1** If the UPT's EPP and the ICC reader are not integrated into the same secure module, and the cardholder verification method (i.e., the IC card requires) is determined to be an enciphered PIN, then the PIN block shall be enciphered between the EPP and the ICC reader using either an authenticated encipherment key of the IC card, or in accordance with ISO 9564.

Guidance

DTRs A1 and D1 verify the physical protections relevant to DTR D4.

It is not acceptable to answer "No" or "N/A" to any option under D4 that is supported by the UPT. As part of this test procedure, the evaluator must verify that the vendor has answered "Yes" to all methods of PIN transmission between the EPP and the ICC reader that are supported by the UPT.

D4 requires that the following be met:

- A plain-text PIN from the EPP to the ICC reader is never permitted except when the EPP and ICC reader are integrated into the same secure module.
- When the cardholder verification method is determined to be an enciphered PIN, the encipherment must occur within the EPP itself or a secure component of the UPT. The PIN must be enciphered in accordance with ISO 9564 for secure transport between the EPP and the secure component.
- Both D4.1 and D4.2 must be complied with for any non-integrated device supporting offline PIN entry.

TD4.1.1 The tester shall examine the vendor's response to Section D4 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D4 of the *PCI UPT Security Requirements* for consistency relevant to D4.1.

TD4.1.2 The tester shall test the device to determine that the PIN is enciphered between the UPT's EPP and the ICC reader using one of the following:

- a) An authenticated encipherment key of the ICC
- b) Triple-DES

Tests that may be performed include: performing a simulated transaction so that PIN data can be captured and analyzed, using a special function of the UPT that allows a user to determine the methods of encryption used, or using test tools (such as ICC emulators) and software to determine the method of encipherment. The tester may require the vendor to supply special hardware and software to facilitate this test, or they can use their own hardware and test tools.

- D4.2** *If the UPT's EPP and the ICC reader are not integrated into the same secure module, and the cardholder verification method is determined to be a plain-text PIN, then the PIN block shall be enciphered from the EPP to the ICC reader (the ICC reader will then decipher the PIN for transmission in plain-text to the IC card) in accordance with ISO 9564.*

Guidance

DTRs A1 and D1 verify the physical protections relevant to DTR D4.

It is not acceptable to answer "No" or "N/A" to any option under D4 that is supported by the UPT. As part of this test procedure, the evaluator must verify that the vendor has answered "Yes" to all methods of PIN transmission between the EPP and the ICC reader that are supported by the UPT.

A plain-text PIN from the EPP to the ICC reader is never permitted except when the EPP and ICC reader are integrated into the same secure module.

Both D4.1 and D4.2 must be complied with for any non-integrated device supporting offline PIN entry.

- TD4.2.1** The tester shall examine the vendor's response to Section D4 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D4 of the *PCI UPT Security Requirements* for consistency relevant to D4.2.
- TD4.2.2** The tester shall test the device to determine that the PIN is enciphered between the UPT's EPP and the ICC reader in accordance with ISO 9564.
Tests that may be performed include: performing a simulated transaction so that PIN data can be captured and analyzed, using a special function of the UPT that allows a user to determine the methods of encryption used, or using test tools (such as ICC reader emulators) and software to determine the method of encipherment. The tester may require the vendor to supply special hardware and software to facilitate this test, or they can use their own hardware and test tools.

- D4.3.** *If the UPT's EPP and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be an enciphered PIN, then the PIN block shall be enciphered using an authenticated encipherment key of the IC card.*

Guidance

DTRs A1 and D1 verify the physical protections relevant to DTR D4.

It is not acceptable to answer "No" or "N/A" to any option under D4 that is supported by the UPT. As part of this test procedure, the evaluator must verify that the vendor has answered "Yes" to all methods of PIN transmission between the EPP and the ICC reader that are supported by the UPT.

Both D4.3 and D4.4 must be complied with for any integrated device supporting offline PIN entry.

- TD4.3.1** The tester shall examine the vendor's response to Section D4 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D1 of the *PCI UPT Security Requirements* for consistency relevant to D4.3
- TD4.3.2** The tester will perform a transaction and capture the encrypted PIN block between the UPT's EPP and ICC reader. The tester may require the vendor to supply special hardware and software to facilitate this test, or they can use their own hardware and test tools.

- D4.4** If the UPT's EPP and the ICC reader are integrated into the same secure module, and the cardholder verification method is determined to be a plain-text PIN, then encipherment is not required if the PIN block is transmitted wholly through a protected environment (as defined in ISO 956). If the plain-text PIN is transmitted to the ICC reader through an unprotected environment, then the PIN block shall be enciphered in accordance with ISO 9564.

Guidance

DTRs A1 and D1 verify the physical protections relevant to DTR D4.

It is not acceptable to answer "No" or "N/A" to any option under D4 that is supported by the UPT. As part of this test procedure, the evaluator must verify that the vendor has answered "Yes" to all methods of PIN transmission between the EPP and the ICC reader that are supported by the UPT.

Both D4.3 and D4.4 must be complied with for any integrated device supporting offline PIN entry.

- TD4.4.1** The tester shall examine the vendor's response to Section D4 of the *PCI UPT Evaluation Vendor Questionnaire* and the response to Requirement D4 of the *PCI UPT Security Requirements* for consistency relevant to D4.4.
- TD4.4.2** The tester shall verify that the plain-text PIN is transmitted wholly through a protected environment. This will be accomplished by examining the UPT to determine that its tamper-detection protections are equivalent to the protections required by D1, and for compliance to ISO 9564.
- TD4.4.3** If the plain-text PIN is transmitted to the ICC reader through an unprotected environment, the tester shall test the device to determine that the PIN is enciphered between the UPT's EPP and the ICC reader in accordance with ISO 9564.
- Tests that may be performed include: performing a simulated transaction so that PIN data can be captured and analyzed; using a special function of the UPT that allows a user to determine the methods of encryption used; or using test tools (such as ICC reader emulators) and software to determine the method of encipherment.

Appendix A: Criteria for the Privacy Screen Design

A.1 Privacy Screen Design Criteria to be Met by the UPT's Design

The following are examples of UPT privacy screens being provided by the UPT itself that are compliant with PCI UPT security requirements. Other designs may also be acceptable.

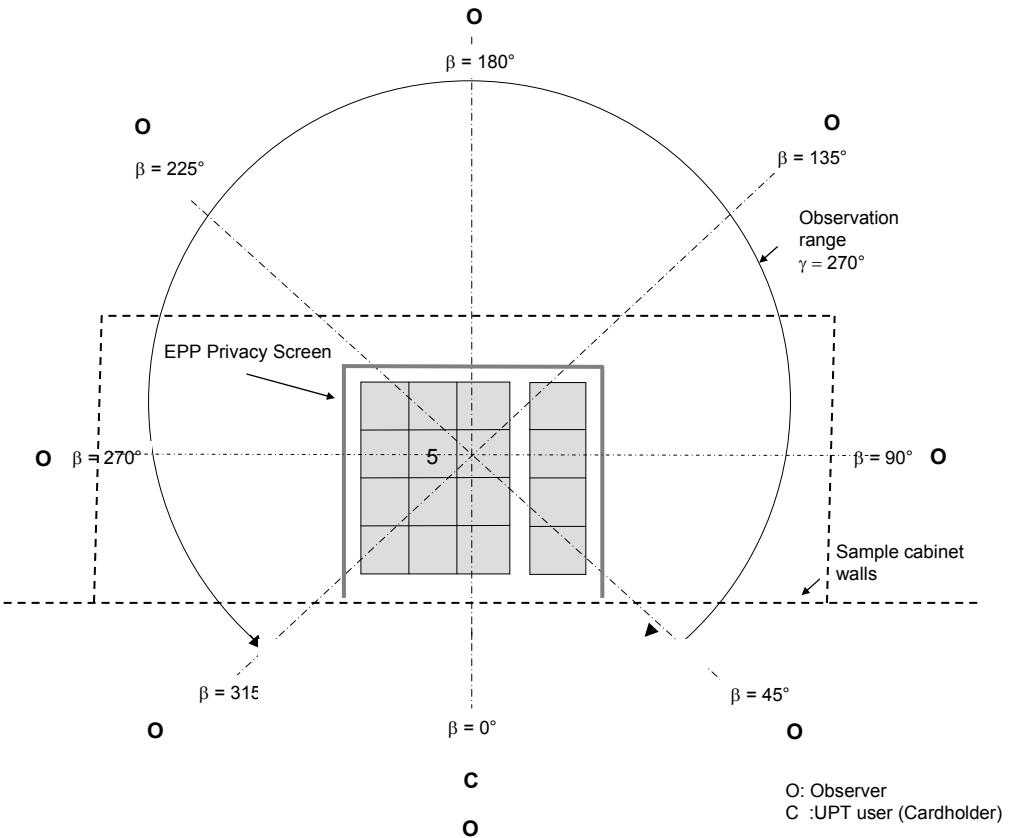


Figure A1: Sample UPT with privacy screen range, bird's eye view

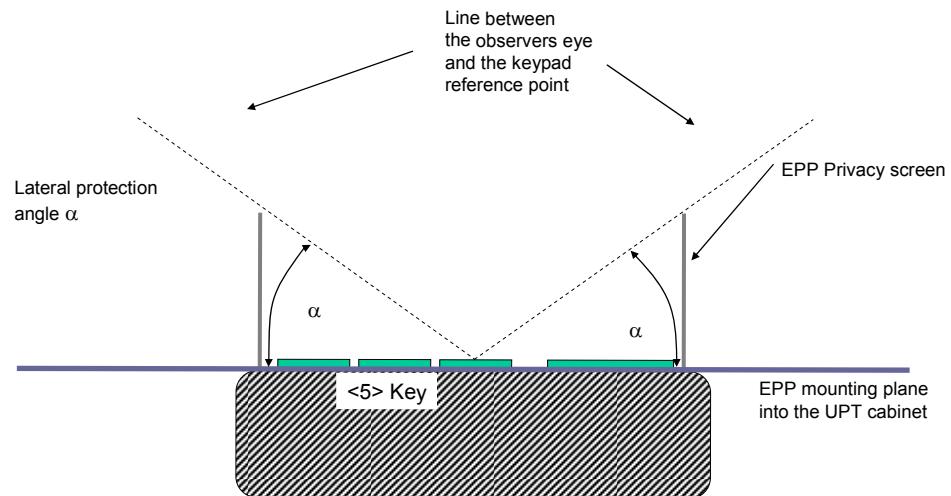


Figure A2: Sample UPT keypad, sectional drawing from the “0” side

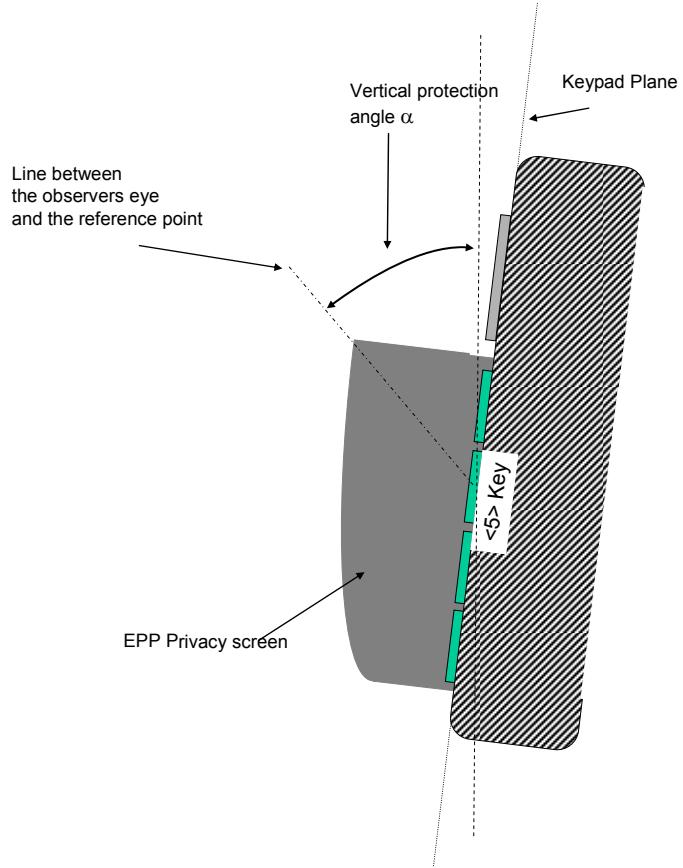


Figure A3: Sample UPT keypad, side view

The angles in the figures above are defined as follows:

- α : Angle between the horizontal plane through the '5' key and a virtual line which connects the '5' key and an observer's eye
- β : Horizontal position of an observer relative to the PED user's position
- γ : Horizontal range which is to be covered by the privacy screen
- δ : Angle between the keypad plane and the horizontal plane

Design rules:

1. These definitions apply to a privacy shield, which is provided as design property by the UPT. It may be a part of the EPP, or provided by the UPT cabinet. The rules and the figures above are to be considered as guidelines, which may be replaced by other means of at least the same efficiency.
2. The keypad reference point is taken as the column position in the middle of the keypad in the row containing the numeric key '5.'
3. The privacy screen shall provide the following protection angles:

Horizontal angle β	Remark	Vertical angle α
$315^\circ \leq b \leq 45^\circ$:	Within this range of β the cardholder deters an observer with her/his body.	N/A
$45^\circ \leq b \leq 90^\circ$ $270^\circ \leq b \leq 315^\circ$:	Within these ranges visual observation of the keypad is partially blocked by the cardholder. The protection angle α shall be at least 35° . Please note that the front end of the privacy screen must be higher if the PED is tilted.	$\alpha \geq 35^\circ$
$90^\circ \leq \square \leq 270^\circ$:	The protection angle shall be at least 40° . The display side of the privacy screen may be lowered as the PED is tilted against the horizontal plane.	$\alpha \geq 40^\circ$

4. The protection is based on viewing angles and does not imply a specific technical implementation like physical shields.

A.2 Privacy Screen Design Criteria to be Met by the UPT's Installed Environment

The following techniques can be employed to provide for effective screening of the PIN-entry keypad during the PIN entry process. These methods would typically be used in combination, though in some cases a method might be used singly.

Note: This option does not preclude the use of privacy mechanisms as defined in A1, but allows less restrictive physical mechanisms, e.g., $\alpha \geq 20^\circ$.

- Positioning of terminal on the check-stand in such way as to make visual observation of the PIN-entry process infeasible. Examples include:
 - Visual shields designed into the check-stand. The shields may be solely for shielding purposes, or may be part of the general check-stand design, e.g., used as selling area.
 - Position the UPT so that it is angled in such a way to make PIN spying difficult.
- Pop-up (temporary) privacy shield attached to the UPT mounting stand. Consumer (through education and prompting) or merchant would put the shield in place during PIN entry
- Installing UPT on an adjustable stand that allows consumers to swivel the terminal sideways and/or tilt it forwards/backwards to a position that makes visual observation of the PIN-entry process difficult.
- Positioning of in-store security cameras such that the PIN-entry keypad is not visible.
- Instructing the cardholder regarding safe PIN-entry. This can be done with a combination of
 - Signage on the UPT;
 - Prompts on the display, possibly with a "click-through" screen;
 - Potentially, literature at the point of sale; and
 - A logo for safe PIN-entry process.

Other methods are possible as well. The above are examples of some of the methods a vendor can propose to protect PINs during PIN entry. The vendor must provide adequate techniques in the UPT documentation and also include a matrix showing which techniques should be used to protect against specific observation corridors. An example matrix follows:

Table A1: Sample Matrix of Observation Corridors and PIN Protection Methods

Method	Observation Corridors				
	Cashier	Customers in Queue	Customers Elsewhere	On-Site Cameras	Remote Cameras
UPT Stand A	M	H	L	L	L
UPT Stand B	H	H	H	L	M
Check-Stand A	L	M	M	L	H
Check-Stand B	H	H	M	H	H
Customer Instruction	H*	H*	H*	H*	H*

* Customer Instruction methods are less repeatable and therefore should be used in combination with other methods.
L = low, **M** = medium, **H** = high.

The matrix must show the purchaser of the UPT, the types of methods they may use to protect their customers' PINs. The appropriate methods would be selected in order to ensure an appropriate level of protection from all observation corridors.

Appendix B: Attack Potential Formula (Adopted from JIL)

Calculating Attack Potentials

This section examines the factors that determine attack potentials and provides some guidelines to help removing some of the subjectivity from this aspect of the evaluation process. This approach should be adopted unless the evaluator determines that it would be inappropriate, in which case a rationale is required to justify the validity of the alternative approach.

Identification and Exploitation

For an attacker wanting to exploit a vulnerability, the vulnerability must first be identified. This may appear to be a trivial separation, but it is an important one. To illustrate this, first consider a vulnerability that is uncovered following months of analysis by an expert, and a simple attack method published on the Internet. Compare this to a vulnerability that is well known but requires enormous expenditure of time and resources to exploit. Of course, factors such as time need to be treated differently in these cases.

Factors to be Considered

The following factors should be considered for the analysis of the attack potentials required to exploit vulnerability:

1. **Identification**
 - a) Attack time for the various levels of expertise;
 - b) Potential to acquire the required knowledge of the UPT's design and operation;
 - c) Potential for the access to the UPT;
 - d) Equipment required like instruments, components, IT hardware, software required for the analysis;
 - e) UPT specific spare components.
2. **Exploitation**
 - a) Attack time for the various levels of expertise;
 - b) Potential to acquire the required knowledge of the UPT's design and operation;
 - c) Potential for the access to the UPT;
 - d) Equipment required like instruments, components, IT hardware, software required for the analysis;
 - e) UPT specific spare components.

In many cases these factors don't depend on each other but might be substituted for each other in varying degrees. For example, expertise or hardware/software can be a substitute for time. A discussion of these factors follows.

The **attack time** is given in the time in hours taken by an attacker to identify or exploit an attack. If the attack consists of several steps, the attack time can be determined and added to achieve a total attack time for each of these steps. The time expired is used for the attack estimation, assuming that a single thread of activities is performed. In those cases where attendance is not required during part of the attack time, the attack time is to be taken as expired time divided by 3. The resulting time is classified as shown in the table below.

Expertise refers to the level of generic knowledge of the application area or product type (e.g., Unix operation systems, Internet protocols). Identified levels are as follows:

- a) **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, etc. implemented in the product or system type and the principles and concepts of security employed;
- b) **Proficient** persons are knowledgeable in that they are familiar with the security behavior of the product;
- c) **Laymen** are unknowledgeable compared to experts or proficient persons, with no particular expertise.

If proficient expertise on various areas of technology is required for an attack, e.g., on electrical engineering and cryptography, an expert level of expertise can be assumed. If an attack requires expert level expertise on various areas of technology, the rating of multiple experts is to be applied.

The level of **Multiple Experts** allows for a situation where an **Expert** level of knowledge, in multiple areas of technology, is required for an attack. The use of **Multiple Experts** must concern fields that are strictly different, e.g., HW manipulation and cryptography. The **Multiple Experts** level pertains to fields of discipline, not the actual number of individuals required for an attack. Strong justification must be provided for the use of the **Multiple Experts** level.

Knowledge of the UPT refers to obtaining specific expertise in relation to the UPT. This is different from generic expertise but not unrelated to it. Identified levels are as follows:

- a) **Public information** about the UPT (or no information): Information is considered public if it can be easily obtained by anyone (e.g., from the Internet) or if it is provided by the vendor to any customer.
- b) **Restricted information** concerning the UPT (e.g., as gained from vendor technical specifications): Information is considered restricted if it is distributed on request and the distribution is registered (e.g., like the *PCI UPT DTRs*).
- c) **Sensitive information** about the UPT (e.g., knowledge of internal design, which may have to be obtained by "social engineering" or exhaustive reverse engineering).

Care should be taken here to distinguish between information required to identify the vulnerability and the information required to exploit it, especially in the area of sensitive information. Requiring sensitive information for exploitation would be unusual.

Specialist expertise and **knowledge of the UPT** are concerned with the information required for persons to be able to attack a UPT. There is an implicit relationship between an attacker's expertise and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to effectively use equipment. Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply—for instance, when environmental measures prevent an expert attacker's use of equipment; or when, through the efforts of others, attack tools requiring little expertise for effective use are created and freely distributed (e.g., via the Internet).

Access to the UPT is also an important factor. It is assumed here that the UPT would be purchased or otherwise obtained by the attacker and that beside other factors there's no time limit in analyzing or modifying the UPT. Differences are defined in the status and functionality of the device to be analyzed or tested. **Mechanical samples** are non-functional and are used merely to study the mechanical design or for supplying spare parts. **Functional samples without working keys** might be used for the logical and electrical behavior of the device but aren't loaded with working keys and are therefore not functional within a payment network or with real payment cards. Such devices might be regularly purchased.

Functional samples with working keys are fully functional devices, which might be used to verify an attack method or to actually perform an attack. If more than one sample is needed in any category, instead of multiplying the points by the number of samples, the following factors must be used:

Table 1: Multiple Samples Factors

Number of Devices	Factor
1	1
2	1.5
3-4	2
5-10	4
>10	5

Equipment refers to the equipment that is required to identify or exploit vulnerability.

- a) **Standard equipment** is equipment that is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment can be readily obtained—e.g., at a nearby store or downloaded from the Internet. The equipment might consist of simple attack scripts, personal computers, card readers, pattern generators, simple optical microscopes, power supplies, or simple mechanical tools.
- b) **Specialized equipment** isn't readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g., dedicated electronic cards, specialized test bench, protocol analyzers, oscilloscopes, microprobe workstation, chemical workbench, precise milling machines, etc.) or development of more extensive attack scripts or programs.
- c) **Bespoke equipment** is not readily available to the public as it might need to be specially produced (e.g., very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive (e.g., Focused Ion Beam, Scanning Electron Microscope, and Abrasive Laser Equipment). Bespoke equipment, which can be rented, can be treated as specialized equipment. Software that has been developed during the identification phase is considered as bespoke equipment; it must not additionally be considered for in the exploitation phase.

Parts refer to components required to hide the signs of an attack; to otherwise replace components that have been broken during an attack, like a case part, a display or a printer; to created data-monitoring or communicating bug; or otherwise are needed to perform the attack. If the same part may be used for identification and exploitation, it must only be accounted for once.

- a) **Standard parts** are readily available to the attacker, either by purchasing them from a supply store or by re-using parts from a mechanical sample of the same device.
- b) **Specialized parts** are not readily available to the attacker but could be acquired without undue effort. These might be parts that can be ordered from the stock but require long delivery time or a certain minimum component count for purchase.
- c) **Bespoke parts** are not readily available and have to be specifically manufactured. It is very unlikely that an attack requires bespoke spare parts.

Multiple Devices

It is intended that the Identification phase of an attack calculation accounts for testing and development of an attack, such that the Exploitation phase of an attack is likely be successful. PCI does not intend multiple devices to be used during the attack phase to account for the probability of success. If multiple devices are included as part of an attack, strong justification must be provided. In all cases, the valid attack scenario(s) with the lowest attack potentials must be presented.

An Approach to Calculation

The above section identifies the factors to be considered. The table below gives guidelines for the individual factors. When a factor falls close to a boundary, the evaluator should consider use of an intermediate value to those in the table.

For a given attack it might be necessary to make several passes through the table for different attack scenarios (e.g., trading off expertise for time or equipment). The lowest value obtained for these passes should be retained. In the case of a vulnerability that has been identified and is in the public domain, the identifying values should be selected for an attacker to uncover that attack scenario in the public domain, rather than to initially identify it.

Table 2: Attack Potential Factors

Factor	Range	Identification Phase	Exploitation Phase
Attack Time	< 1 hour	0	0
	<= 1 day	1	2
	<= 1 week	2	3
	<= 1 month	3	4
	> 1 month	5	7
Expertise	Layman	0	0
	Proficient	1	1
	Expert	2	3
	Multiple Expert	5	6
Knowledge of the UPT	Public	0	0
	Restricted	2	2
	Sensitive	3	4
Access to the UPT per unit required for the attack. <i>Note: If more than one unit is required in any category, the values must be multiplied by the factors given above.</i>	Functional samples without working keys	2	2
	Functional sample with working keys and software	4	4
	Mechanical sample	1	1
Equipment required for the attack	None	0	0
	Standard	1	2
	Specialized	3	4
	Bespoke	5	6
Specific parts required	None	0	0
	Standard	1	1
	Specialized	2	2
	Bespoke	4	4

An approach such as this cannot take account of every circumstance or factor but should give a better indication of the attack potential. Other factors, such as the reliance on unlikely chance occurrences or the likelihood of detection before an attack can be completed, are not included in the basic model but can be used by an evaluator as justification for a rating other than those that the basic model might indicate.

First Attack Example

The attack aims to insert a PIN-disclosing bug into a UPT. The bug is placed at a position in the device where the PIN is handled in clear, for instance at the keypad or at the ICC reader interface. It is assumed that such an attack is possible. A generic attack consists of the following steps:

1. Reverse-engineer the device and develop the attack models. This step requires professional knowledge of electronic engineering and the capability to perform the mechanical and electronic test required. The modules will break during that phase. It is assumed that the device is protected by tamper-response circuits, which prevent undetected opening of the device, but the points of interest are not covered by a tamper-responsive envelope.
2. The tamper-detection measures have to be deactivated.
3. A PIN-disclosing bug is placed into the UPT (Exploitation Phase).
4. The sensitive data is collected from the UPT.

We assume that more than one sample of the device is needed for the identification phase but only the target device is required for the exploitation phase of the attack. The skill level required is Expert. The same standard equipment is used and required at identification and exploitation time. The following table consists of references to the attack phases.

Table 3: Attack Potential for Inserting a PIN-Disclosing Bug

Aspect	Identifying Value	Exploiting Value		
Attack time	≤ 1 week	2	≤ 1 day	2
Expertise	Expert	2	Expert	3
Knowledge of the device	Restricted	2	Public	0
Access to UPT	Two functional samples w/o target keys	3	Functional sample with working keys	4
Equipment	Standard	1	Standard	2
Specific parts	Standard	1	No further parts required	0
Attack potential per phase		11		11
Total Attack Potential			22	

Second Attack Example

The attack aims at the determination of a DES key used for encryption at the device using differential power analysis (DPA). It is assumed that:

- A function of the UPT is used which requires a PIN to be entered for every execution of the cryptographic action with the key under attack;
- The data used for DPA can be acquired at an external interface of the UPT module, e.g., the UPT needs not be further physically attacked to get the required test data; and that
- The attacked UPT module does not have effective countermeasures against DPA.

The attack would consist of the following steps:

1. Determine the method to run DPA on a UPT. This consists mostly of analyzing the electrical and logical interfaces to the UPT and/or the UPT's modules. This step requires expert knowledge of electronic and computer engineering.
2. Develop the attack set-up including the control to run the UPT module under attack in an automated way. Since a large number of PIN entries are required, which can hardly be performed manually, special mechanics must be developed to perform the PIN entries. This is bespoke equipment, developed specially for this attack, which will be reused at Identification time. Also, the data-analyzing software must be considered as bespoke equipment.
3. Get a UPT and perform the measurement. We expect that at least 20,000 PIN entry steps and the following encryption have to be observed. In the identification phase, this may have to be repeated several times. Due to the exhaustive PIN search countermeasure, 20,000 PIN entries need at least seven days. Since such an amount of transactions cannot be performed in a real live environment, it must be possible to run the device off-line with a simulated host.
4. Analyze the data samples and retrieve the PIN-encrypting key.

The attack potentials are estimated within the following table:

Table 4: Attack Potentials Example for DPA Analysis

Aspect	Identifying Value		Exploiting Value	
Attack time	> 1 month	5	< 1 month	3
Expertise	Expert	2	Expert	3
Knowledge of the device	Restricted	2	Public	0
Access to PED	Functional sample with trial keys	2	Functional sample with working keys	4
Equipment	Bespoke	5	Specialized	4
Specific parts	Standard	1	No further parts required	0
Attack potential per phase		17		14
Total Attack Potential			31	

As can be seen from the table, the attack potential is below the margin of 35 for the attack potential high level. If a key can be attacked which does not require the entry of a PIN at the keypad and the attack time is less than a day, the attack potential is even lower.

Appendix C: Configuration and Use of the sts Tool

The tester should compile and/or install NIST's sts tool (the reference implementation of the SP800-22 test set) and then test this instance of the sts tool tested as per SP800-22, Appendix C to verify that the tool is functioning correctly on the testing platform. This configuration guidance is for use with sts versions 1.5 through 1.8.

A note on sts versions: Prior to version of 1.7, the Discrete Fourier Transform (Spectral) test was conducted using the incorrect peak height threshold value (called T in Section 2.6.4 of SP 800-22) and calculated the normalized difference (d) incorrectly. In order to use an older version of the sts tool, the corrections described in [Kim 2004] should be implemented for this test. In versions 1.7 and later, these corrections are already included.

The tester should request and obtain a sample of 2^{30} bits from the vendor. The tester should exercise care to verify that the vendor-supplied data is interpreted correctly by the sts tool (the sts tool assumes that binary data is in big-endian formatting on all platforms).

All tests other than the Lempel-Ziv test should be run [0] (for later versions of sts, the Lempel-Ziv test is normally inaccessible).

The sts testing on the data shall be judged as a "pass" if it passes all of the tests, for both the "Proportion of Sequences Passing a Test" interpretation approach and "Uniform Distribution of P-Values" interpretation approach. If the data does not pass all tests, and the failure is marginal, the tester should acquire additional data from the vendor and repeat the testing, including both the initial data and the additional vendor-supplied data.

The sts tool should be configured as per guidance provided in SP800-22, which is summarized below.

The following settings are consistent with the SP800-22 document:

Configuration Item	Setting
Length of bit streams (n)	1,000,000 [1]
Number of bit streams (sample size) (M)	1,073 [2]
Block Frequency block length	20,000 [3]
Non-Overlapping Templates template length	10 [4]
Overlapping Template template length	10 [4]
Universal block length (L), number of initialization steps (Q)	$L=7$, $Q=1,280$ [5]
Approximate Entropy block length	8 [6]
Serial block length	16 [7]
Linear Complexity block length	1,000 [8]

- [0] The Lempel-Ziv test should be excluded due to an error in the test, as described in [Kim 2004]. NIST has acknowledged the error and the Lempel-Ziv test has been dropped from recent versions of the sts tool.
- [1] n must be selected to be consistent with the requirements all of the tests to be run. The Overlapping Templates, Linear Complexity, Random Excursions, and Random Excursions Variant tests all require n to be greater than or equal to 10^6 in order to produce meaningful results. The Non-Overlapping Templates test requires n to equal 10^6 . (See SP800-22 Sections 2.7.7, 2.8.7, 2.10.7, 2.11.7, 2.15.7, and 2.16.7)
- [2] The number of bit sequences (sample size) must be 1,000 or greater in order for the "Proportion of Sequences Passing a Test" result to be meaningful. (See SP800-22 Sections 4.2.1 and 4.3 f.) This value will be 1,073 for the first test, but any additional testing (e.g., further testing to resolve test failures) will necessarily include more bit sequences.
- [3] For the Block Frequency Test, if $n=10^6$, the test block size should be set between 10^4 and 10^6 . (See SP800-22 Section 2.2.7.)
- [4] The two template tests (Non-Overlapping and Overlapping tests) both require selection of a template length of 9 or 10 in order to produce meaningful results. (See SP800-22 Sections 2.7.7 and 2.8.7.)
- [5] The Universal test block length (L) and initialization steps (Q) must be consistent with the table in SP800-22 Section 2.9.7. For $n=10^6$, the only acceptable values are ($L=6$, $Q=640$) and ($L=7$, $Q=1280$).
- [6] For the Approximate Entropy (ApEn) test, SP800-22 Section 2.13.7 requires the block length to be less than $\lfloor \log_2 n \rfloor - 2$, however the sts tool warns if the block size is greater than $\lfloor \log_2 n \rfloor - 5$ (which is consistent with the information in Section 4.3 f). Other analysis [Hill 2004] has shown that for $n=1,000,000$ values block lengths greater than 8 can cause failures more often than expected for large scale testing.
- [7] The Serial Test block length is also set based on n . If $n=10^6$, the block length must be less than 17. (See SP800-22 Section 2.12.7)
- [8] The Linear Complexity Test block length is required to be set to between 500 and 5,000 (inclusive), and requires that $\frac{n}{M} \geq 200$. (See SP800-22 Section 2.11.7.)

References

- [Rukhin 2001] Rukhin, Andrew, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST SP800-22, revisions dated May 15, 2001.
- [Rukhin 2004] Rukhin, Andrew (NIST). E-Mail correspondence regarding Kim, et al paper.
- [Kim 2004] Kim, Song-Ju, et al., "Corrections of the NIST Statistical Test Suite for Randomness".
- [Bassham 2004] Bassham, Larry (NIST). "Validation Testing and NIST Statistical Test Suite" presentation dated July 22, 2004.
- [Hill 2004] Hill, Joshua (InfoGard Labs). "ApEn Test Parameter Selection".