**Terminal Manufacturers**

**PCI PTS labs**

**Terminal Vendors**

**Security design for terminals, encrypting PIN pads and encrypting card readers**

**Best Practice: Security Design - Ver B Final**

Type: Security

11 June 2013

|  |
| --- |
| The terminal manufacturers ensure that:* Terminals fulfil the Visual shield and keyboard layout requirements found in the following two documents Visual Shield and Keyboard Layout.
* Terminals, encrypting PIN pad and encrypting card readers are assessed by a PCI PTS lab according to this document.

The objectives are to prevent visual observation of PIN being entered by the cardholder and to get information about the product design.The terminal manufacturer is requested to provide the information needed for a PNC SAC review presented under the title *Requested information from the review*. The PCI PTS lab can use their own report format or use applicable parts of the forms section of this document. If the later one is used, the forms part, i.e. page 4 and onwards, is sent as a pdf to PNC after it has been completed. PNC lists Terminals, encrypting PIN pads and encrypting card readers that have been validated to fulfil the security design requirements on [List 6](http://www.pan-nordic.org/Renderers/ShowMedia.ashx?id=0d7910ed-bf22-49ab-8cb0-043914e794fd). |

# Version history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description  | Issued/revised by |
| 2011-10-14 | A Final | A new document  | PNC SAC |
| 2013-06-11 | B Final | Tables according to PCI PTS ver 4. | PNC SAC |

# Definitions

PNC SAC uses in this document the PCI PTS Definitions from the documents:

* (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, Version 4.0)
* (Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide Version 1.2)

# Related documents

“**Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide Version 1.2.**” July 2012. 11 June 2013 <https://www.pcisecuritystandards.org/documents/PTS\_Program\_Guide\_01Jul12.pdf>.

“**Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, Version 4.0.**” June 2013. 11 June 2013 <https://www.pcisecuritystandards.org/documents/PCI\_PTS\_POI\_SRs\_v4\_Final.pdf>.

“**Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 4.0**.” June 2013.

# Requested information from the review

1. **Manufacturer and product details**

For each device, the PCI PTS lab shall provide PNC SAC with:

* Device Manufacturer information according to table 1. Please see the forms section.
* Device Information according to page 8, 10, 11 and 12 in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, Version 4.0)
* The PCI PTS Approval number
* Configuration Information according to Table 7 in the forms section

# Information on product design

The following areas shall at least be covered:

* 1. A high-level description with pictures of the IT product and its major components based on the deliverables required for the PCI approval. The pictures should at least show:
		1. **Picture 1**: The front view
		2. **Picture 2**: The physical access ports of the terminal
	2. Requirements for the product placement (for example, stand, checkout counter mounted, handheld together with Personal Digital Assistant (PDA), handheld and unattended payment terminal). All possible alternatives are to be described.
	3. For the privacy shielding[[1]](#footnote-1), the following should at least be presented:
		1. The POS POI Terminal’s dimensions are to be presented according to the **Table 8** in the forms section.
		2. **Picture 3**[[2]](#footnote-2): A picture of the POS POI terminal with the visual shield
		3. A table presenting: 1) the measured vertical angles α, 2) the required vertical angles α according to Appendix A in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 4.0) and 3) a conclusion for each different horizontal angle β. The result is presented according to **Table 9[[3]](#footnote-3)** in the forms section.
		4. A conclusion that the visual shield fulfils the visual shield requirements in Appendix A in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 4.0).[[4]](#footnote-4)
1. **Manufacturer and product details**

|  |
| --- |
| **Table 1: Device Manufacturer Information** |
| **Company Name:** |       |
| **Business Address:** |       |
| **City:** |       | **Postcode:** |       |
| **Country:** |       |
| **Contact Person:****(printed on approval)** |       |
| **Telephone:** |       | **E-mail:** |       |
| **Website:** |       |

|  |
| --- |
| **Table 2: Required Device Information** |
| **Device type claim** | **POS terminal containing a PIN entry device (select one):** |
| [ ]  Dedicated for PIN entry only | [ ]  UPT (Vending, AFD, Kiosk) |
| [ ]  Stand-alone POS terminal | [ ]  Other |
| [ ]  **Encrypting PIN pad (for ATM, Vending, AFD or Kiosk)** |
| [ ]  **Secure (encrypting) card reader** |
| [ ]  **Other secure component for PIN entry device**  |
| [ ]  **Non-PED POI device**  |
| **Manufacturer** |       |
| **Marketing Model Name/Number** |       |
| **Hardware VersionNumber:** |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Use of “x” represents a variable field | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| **Software VersionNumber:** |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Use of “x” represents a variable field | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| **Application VersionNumber:** (if applicable) |       |
| **Version of PCI PTS POI Security Requirements:**  | V4 | FAQ version:       |
| **PCI PTS ApprovalNumber:** |       |
| **Validation modules required**  |  | **Yes** | **No** | **N/A** |
| Core PIN Entry Security  | [ ]  | [ ]  | [ ]  |
| POS Terminal Integration  | [ ]  | [ ]  | [ ]  |
| Open Protocols  | [ ]  | [ ]  | [ ]  |
| Secure Reading and Exchange of Data  | [ ]  | [ ]  | [ ]  |
| Other  |       |
| **Previously Approved Components Used\* (if applicable)** |
| **Vendor Name** | **Device Marketing/Model Name** | **PCI PTS Approval Number** | **Expiry Date** | **Product Type per PCI SSC Website** | **Other** |
|       |       |       |       |       |       |
|       |       |       |       |       |       |
|       |       |       |       |       |       |

|  |
| --- |
| **Table 3: Optional Use of Variables in the Identifier**  |

Please provide a table that is providing information on the optional use of variables in the hardware version number[[5]](#footnote-5) and the firmware version number.

**Hardware Version Number – The use of the Variable “x”**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|  |  |
| --- | --- |
| **Variable “x” Position** | **Description of Variable “x” in the Selected Position** |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |

**Firmware Version Number – The use of the Variable “x”**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

|  |  |
| --- | --- |
| **Variable “x” Position** | **Description of Variable “x” in the Selected Position** |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |
|       |       |

|  |
| --- |
| **Table 4: Evaluation Module Information[[6]](#footnote-6)** |
| **PIN support** | [ ]  | N/A (explain)       |
| [ ]  | Offline only  |
| [ ]  | Offline and Online  |
| [ ]   | Online only |
| **Key Management:** | [ ]   | N/A (explain)       |
| [ ]   | DUKPT |
| [ ]   | Fixed |
| [ ]   | MK/SK |
| **PIN entry technology** | [ ]   | N/A (explain)       |
| [ ]   | Physical (Hard) Keys |
| [ ]   | Touch screen |
| [ ]   | Other |
| **Prompt Control** | [ ]  | N/A (explain)       |
| [ ]  | Acquirer-controlled  |
| [ ]  | Terminal manufacturer-controlled |
| [ ]  | Other (explain)       |
| **Other Functions provided** | [ ]  | Display |
| [ ]  | CTLS |
| [ ]  | ICCR |
| [ ]  | MSR |
| [ ]  | OP |
| [ ]  | SRED |

**Table 5: Open Protocol Module – Protocol**

Please complete if the validation module was required.

|  |  |  |
| --- | --- | --- |
| **Link Layer Protocols** | [ ]  | Yes |
| [ ]  | No  |
| [ ]  | N/A  |
| Name:       |
| **IP Protocols** | [ ]  | Yes |
| [ ]  | No  |
| [ ]  | N/A  |
| Name:       |
| Number:       |
| **Security Protocols** | [ ]  | Yes |
| [ ]  | No  |
| [ ]  | N/A  |
| Name:       |
| **IP Services** | [ ]  | Yes |
| [ ]  | No  |
| [ ]  | N/A  |
| Name:       |
| Port Number:       |

**Table 6: Secure Reading and Exchange of Data Module**

Please complete if the validation module was required.

|  |  |  |
| --- | --- | --- |
| **Does the terminal utilise secure reading and exchange of data?** | [ ]  | Yes |
| [ ]  | No  |
| [ ]  | N/A (explain)       |

|  |
| --- |
| **Table 7 - Configuration** |
| **Printer** |       |
| **Communication Method** |       |
| **Interfaces** |       |
| **EMV Level 1** |       |
| **EMV Level 1 Approval Number** |       |

1. **Information on the product design**

**High-level description**

A high-level description with pictures of the product and its major components based on the deliverables required for the PCI approval shall be provided. The pictures should at least show:

**Picture 1**: The front view

**Picture 2**: The physical access ports of the terminal

High-level description with references to the pictures below:

****

**Picture 1:** The front view

****

**Picture 2**: The physical access ports of the terminal



**Picture 3**:



**Picture 4**:

**Requirements for the product placement**

Requirements for the product placement (for example, stand, checkout counter mounted, handheld together with Personal Digital Assistant (PDA), handheld and unattended payment terminal) are to be described. All possible alternatives are to be included.

Description of the requirements for product placement:

**Privacy shielding (only applicable for PIN devices)**

The POS POI Terminal’s dimensions are presented in **Table 8** below.

|  |  |
| --- | --- |
| **Table 8 - Dimensions** |  |
| **Criteria** | **Measured** | **Requirement** |
| Weight |       | ≤ 500 g |
| Height at the ‘5’ key |       |  |
| Width at the ‘5’ key |       | ≤ 7.62 cm (3 inches) |
| Keypad length |       | ≤ 10.16 cm (4 inches) |
| Sum of width and height at the ‘5’ key |       | ≤ 10.16 cm ( 4 inches) |



**Picture 5**: The POS POI terminal with the visual shield

**Table 9** below presents: 1) the measured vertical angles α, 2) the required vertical angles α according to Appendix A in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 4.0) and 3) a conclusion for each different horizontal angle β.

|  |
| --- |
| **Table 9 - Measured angles and conclusion** |
| **Horizontal angle β** | **Vertical angle α (required)** | **Vertical angle α (measured)** | **Conclusion** |
| 315$°$ ≤ β ≤ 45$°$ |       |       |       |
| 45$°$ ≤ β ≤ 90$°$ |       |       |       |
| 90$°$ ≤ β ≤ 270$°$ |       |       |       |
| 270$°$ ≤ β ≤ 45$°$ |       |       |       |

A conclusion that the visual shield fulfils the visual shield requirements in Appendix A in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Derived Test Requirements, Version 4.0)[[7]](#footnote-7) is presented below:

1. All POS POI Terminals exceeding the following requirement are considered not truly-handheld and are to have a privacy shielding:

|  |  |
| --- | --- |
| **Criteria** | **Requirement** |
| Weight | ≤ 500 g |
| Height at the ‘5’ key |  |
| Width at the ‘5’ key | ≤ 7.62 cm (3 inches) |
| Keypad length | ≤ 10.16 cm (4 inches) |
| Sum of width and height at the ‘5’ key | ≤ 10.16 cm ( 4 inches) |

If the device’s properties clearly fall outside these ranges, it will not be accepted as a handheld device. A handheld device must by its size and case shape encourage its handheld use. Being small may not be sufficient. Even if the device is small, if the standing and/or mounting support indicate that the PIN entry device is to be installed on a swivel arm or a similar apparatus, it will be considered as a desktop device. [↑](#footnote-ref-1)
2. Only applicable if the device is not truly-handheld. [↑](#footnote-ref-2)
3. Only applicable if the device is not truly-handheld. [↑](#footnote-ref-3)
4. Only applicable if the device is not truly-handheld. [↑](#footnote-ref-4)
5. Hardware # represents the specific hardware component set used in the approved payment security device. The fields that make up the Hardware # may consist of a combination of fixed and variable alphanumeric characters. A lower case "x" is used by PCI to designate all variable fields. The "x" represents fields in the Hardware # that the vendor can change at any time to denote a different device configuration. Examples include: country usage code, customer code, communication interface, device colour, etc. [↑](#footnote-ref-5)
6. Please see Table 4 in Appendix A in (Payment Card Industry (PCI) PIN Transaction Security (PTS) Device Testing and Approval Program Guide Version 1.2) for details. [↑](#footnote-ref-6)
7. Only applicable if the device is not truly-handheld. [↑](#footnote-ref-7)