**Exterior Shield Vendors**

**Terminal vendors**

**Third-Party Auditor**

Exterior Shield

**Best Practice: Exterior Shield - Ver H FINAL**

Type: Security

13 April 2021

|  |
| --- |
| **Exterior Shield**  An Exterior Shield is a part of an Unattended Payment Terminal (UPT) which is a self-service device where the cardholder can perform card payments.      Touch display  Receipt printer  Encrypting Contact/­contactless Card Reader  Encrypting PIN PAD  Exterior/Shield    Trådløs  UPT consists of three different parts:   * The UPT components (card reader, encrypting PIN PAD, etc) * The UPT software (for touch display, receipt printer, etc.) * An exterior shield   **NOTE!** To guarantee that the merchant has a compliant UPT, all the three parts of the UPT that the merchant uses needs to be listed under validated products on the PNC web site at all time. The merchant’s PCI DSS compliance and security are at risk if any part is not listed. The lists on the PNC website ([Validated Products](http://www.pan-nordic.org/PanNordicCard/PCI-and-Security/Validated-Products.aspx)) are:   * [List 3](https://www.pan-nordic.org/security/validated-products/): Secure UPT components for unattended environments (based on the PCI PTS programme) * [List 4](https://www.pan-nordic.org/security/validated-products/) : UPT software that does not handle any cardholder data (no cardholder data handling, based on PCI P2PE or PNC E2EE solutions) * [List 5](https://www.pan-nordic.org/security/validated-products/) : Secure exterior shield (Exterior Shield)   The processes to get products listed on List 3 and List 4 are presented on the PNC website. The process to get products listed on List 5 is presented in this document. |

**Table of Contents**

[1 Purpose of this Best Practice and Form 3](#_Toc11765297)

[2 Validation Process 3](#_Toc11765298)

[2.1 The Exterior Shield Vendor 3](#_Toc11765299)

[2.2 The QSA (Third-Party Auditor) 3](#_Toc11765300)

[3 When must Exterior Shield be revalidated? 3](#_Toc11765301)

[4 Risks and Countermeasures 4](#_Toc11765302)

[5 For further information 4](#_Toc11765303)

[6 Form: Attestation of Compliance 5](#_Toc11765304)

[6.1 Exterior Shield Vendor and product details 5](#_Toc11765305)

[6.2 Exterior Shield Vendor Self-Assessment Questionnaire and Third-Party report of Validation 8](#_Toc11765306)

[6.3 Anti-skimming Questionnaire 10](#_Toc11765307)

[6.4 Vendor Attestation of Compliance 12](#_Toc11765308)

[6.5 Third-Party Auditor Attestation of Validation 12](#_Toc11765309)

Reference list

|  |  |  |
| --- | --- | --- |
| **Ref no.** | **Name of reference** | **Document owner** |
| 1. | [Information Supplement: Skimming Prevention – Best Practices for Merchants](https://www.pcisecuritystandards.org/documents/Skimming_Prevention_BP_for_Merchants_Sept2014.pdf?agreement=true&time=1560858059474) | PCI |
| 2. | [Payment Card Industry (PCI PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements](https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_SRs_v5-1.pdf?agreement=true&time=1559034875695) | PCI |
| 3. | [Best Practice: Visual Shield](https://www.pan-nordic.org/security/register-for-validation/) | PNC |

# Purpose of this Best Practice and Form

The purpose of this Best Practice and Form is to explain the process of how and when to validate Exterior Shield, and document the Exterior Shield including UPT components, UPT software and PIN privacy shield for an Unattended Payment Terminal.

For non-PIN UPTs, this Form is only used for documenting the components and software used.

By using this Best Practice and Form, the Exterior Shield Vendor confirms that:

* Their terminal/components do not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the hardware payment terminal.
* Their terminal/components do not store any cardholder data in electronic format, including no legacy storage of cardholder data from prior payments.
* Their PIN privacy shield does fulfil the measurements required.

Please note that all UPT terminals that do not operate in a transport or parking environment must support PIN or support contactless-only acceptance.

# Validation Process

## The Exterior Shield Vendor

1. Selects listed terminal components from [List 3](https://www.pan-nordic.org/security/validated-products/).
2. Checks that the software version for the terminal components is listed on [List 3](https://www.pan-nordic.org/security/validated-products/)
3. Requests the payment terminal components vendor (terminal vendor) to complete Part 4.
4. Makes sure that the Exterior Shield fulfils the PIN privacy shield requirements and is validated by a [Third-Party Auditor](https://www.pan-nordic.org/security/validated-products/).
5. Provides a clear jpeg picture, 320x320 pixels of the front of the final exterior shield (the picture will be used for [List 5](https://www.pan-nordic.org/security/validated-products/)).

## The QSA (Third-Party Auditor)

1. Assesses the information in all parts of this Form.
2. Confirms and documents by performing measurement that the Exterior Shield fulfils the PIN privacy shield requirements according to PNC Best Practice: Visual Shield.

All parties must complete and sign the Form before the Third-Party Auditor scans and sends the Form (chapter 6) in PDF format to PNC ([validation (at) pan-nordic.org](mailto:validation@pan-nordic.org)) including the documents H01 - H04,

Please note that PNC performs quality assurance before listing, to ensure that the Third-Party Auditor accurately and thoroughly have verified, and documented measurements of the PIN privacy shield and that information provided by the Exterior Shield Vendor is correct.

# When must Exterior Shield be revalidated?

In cases where the UPT components such as: card readers, touch display, etc. are changed, added or modified, will require a revalidation.

Any modification of the Exterior Shield, including change of colour, must be validated. Normally, this means that the daily inspection guide for the merchant is updated to show the new the appearance and that the version number are changed. New manuals for daily inspections and pictures for the listing shall be provided together with the Form, as part of the Exterior Shield revalidation

# Risks and Countermeasures

The main risks connected to Exterior Shield and UPTs are that PIN is noticed together with the card data or the card is stolen. The five main attack scenarios are described below.

1. **Sniffer** **device** **inside** **the Exterior Shield**
   * A sniffer device is used to intercept and to log the traffic from the UPT.
2. **Shoulder-surfing**
   * A pickpocket notices the PIN and pickpockets the card.
3. **Overlay attack -** **Additional card reader together with camera**
   * An additional card reader is installed on top of the original card reader. The additional reader reads the card while it is dragged into the original reader. A camera is also installed in the PIN privacy shield or in the roof.
4. **Overlay attack -** **Additional card reader together with additional PIN keyboard**
   * Like above, an additional card reader is installed on top of the card reader. An extra PIN keyboard or overlay is installed on top of the original PIN-keyboard.
5. **Malware** **in** **the** **PC**
   * Malware is installed within the PC’s UPT software.

Much fraud can be avoided if the cardholder and the merchant staff are vigilant and have got information on how to distinguish modified Exterior Shield from the original Exterior Shield and if the cardholder is informed to protect the PIN.

# For further information

Please contact PNC: validation (at) pan-nordic.org

# 

# Form: Attestation of Compliance

## Exterior Shield Vendor and product details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Part 1: Exterior Shield Vendor information** | | | | |
| Company Name: |  | | | |
| Contact Name: |  | | Title: |  |
| Telephone: |  | | E-mail: |  |
| Business Address: |  | | | |
| Country: |  | | Postcode: |  |
| Organisation/VAT number: |  | | City: |  |
| URL: |  | | | |
|  | | | | |
| **Part 2: Product information for the Exterior Shield** | | | | |
| Product name/model: | |  | | |
| Version: | |  | | |
| Main industry for customers: | | Please select main industry for your customers! | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Part 3: The Exterior Shield documentation** | | | |
| ID | Document name | Version | Date, Time – Modified |
| H01 | Company Name Model Version - Daily Inspections |  | 20  -  -  ,   : |
| H02 | Company Name Model Version – Check List for detecting modifications |  | 20  -  -  ,   : |
| H03 | Photo of the front of the final exterior shield in jpeg, at least 320x320 pixels |  | 20  -  - |
| H04 | The name of the terminal Component Vendor’s document |  | 20  -  -  ,   : |

|  |  |
| --- | --- |
| **Part 4: Product information for the UPT Components** | |
| Supported Card Schemes/Brands: | Visa,  Mastercard,  Dankort  BankAxept  Other Brands | |
| PIN support: | Yes  No -  Contactless /  MCC: | |
| **4.1 – Secure Card Reader (SCR)** | | |
| Manufacturer name: |  | |
| SCR model: |  | |
| Hardware version: |  | |
| Software version: |  | |
| PNC-reference (see List 3): |  | |
| **4.2 – Contactless Secure Card Reader (SCR)** | | |
| Manufacturer name: |  | |
| SCR model: |  | |
| Hardware version: |  | |
| Software version: |  | |
| PNC-reference (see List 3): |  | |
| **4.3 – Encrypting PIN Pad (EPP)** | | |
| Manufacturer name: |  | |
| EPP model: |  | |
| Hardware version: |  | |
| Software version: |  | |
| PNC-reference (see List 3): |  | |
| **4.4 – Other Secure Cryptographic Device (SCD), please specify:** | | |
| Manufacturer name: |  | |
| Device model: |  | |
| Hardware version: |  | |
| Software version: |  | |
| PNC-reference (see List 3): |  | |
| **4.5 – Software** | | |
| **Payment Application information** | | |
| Software name and version for Payment Application | Vendor:  Name:       Version: | |
| PCI PA-DSS approval number or  PCI SSF Validated Payment Software Ref # | -  .     .     . | |

## 

## Exterior Shield Vendor Self-Assessment Questionnaire and Third-Party report of Validation

| **Best Practice #** | **Requirement** | **The Exterior Shield Vendor Self- Assessment Questionnaire (completed by the Exterior Shield Vendor specified in Part 1 of this document)** | **The** **Third-Party Report of Validation (completed by the Third-Party Auditor)** |
| --- | --- | --- | --- |
| 1 | The privacy shield fulfils the PNC requirements in PNC: Best Practice Visual Shield | **Alternative 1:**  **In place** and implemented according to the PNC Best Practice Visual Shield. The Visual Shield Design Criteria is met by the Device’s Design. Measures are:   |  |  | | --- | --- | | **Angle β** | **Measured α** | | 315° ≤ β ≤ 45° |  | | β = 50° |  | | 45° ≤ β ≤ 90°  270° ≤ β ≤ 315° |  | | β = 310° |  | | 90° ≤ β ≤ 270° |  |   **Alternative 2:**  **In place,** the Visual Screen Design Criteria is met by the Device’s Installed Environment. We have provided adequate techniques in the device documentation and included a matrix showing which techniques must be used to protect against specific observation corridors H0X.  **Alternative 3:**  **Not applicable.** (This option is only applicable for non-PIN UPTs.) | **Alternative 1, Option A:**  **In place**, I have verified by visually inspecting the end product that the visual shield design Criteria is met by the Device’s Design to fulfil the Requirement no. 1. Measures are:   |  |  | | --- | --- | | **Angle β** | **Measured α** | | 315° ≤ β ≤ 45° |  | | β = 50° |  | | 45° ≤ β ≤ 90°  270° ≤ β ≤ 315° |  | | β = 310° |  | | 90° ≤ β ≤ 270° |  |   **Alternative 1, Option B:**  **In place**, I have verified by receiving a Visual Shield Letter of Approval issued by a Third-Party Auditor accredited by PNC. The Letter of Approval states the visual shield complies with PNC Best Practice Visual Shield.  **Alternative 2:**  In Place, I have validated that the Visual Screen Design Criteria is met by the Device’s Installed Environment. The Terminal Vendor has provided adequate techniques in the device documentation and has included a matrix showing which techniques must be used to protect against specific observation corridors H0X.  **Alternative 3**:  **Not applicable**, I have verified that the UPT fulfils all the requirements for being a non-PIN UPT. |
| 2 | The product specified in Part 4 is E2EE-validated by PNC and PA-DSS certified or validated and listed by PCI as a P2PE solution. | **Alternative 1:**  **In place**, the product specified in Part 4 is E2EE-validated and exactly the same version can be found on PNC’s list of End-to-End Encryption validated products. Exactly the same version is used in the exterior shield and the following details are exactly the same:   1. Terminal Vendor 2. Manufacturer Name 3. Terminal Model 4. POS Hardware Version 5. Software Version for POS Security Application 6. PED Hardware Version 7. Software Version for PED Security Application 8. PCI PTS Approval number(s) 9. PTS Approval Version 10. Software version for the Payment application 11. Intended Environment 12. PSPs or Member Processors 13. E2EE Validation Date   **Payment Software, Option A**:  **In place**, the software version for the Payment application is found on PCI SSC’s list of PA-DSS-validated payment applications and the Reference # for the PA-DSS Validated Payment Application is exactly the same in Part 4 and on the PCI SSC’s list of PA-DSS-validated payment applications.  **Payment Software, Option B:**  **In place**, the software version for the Payment application is compliant with PCI Secure Software Standard (SSF Validated Payment Software) and the Reference # for the SSF Validated Payment Software is exactly the same in Part 4 and on the PCI’s list of SSF Validated Payment Software.  All secure components used in the exterior shield are listed on [PCI PTS website](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices):  Secure Card Reader  **In place**  **Not in place**  Contactless Secure Card reader  **In place**  Not i**n place**  Encrypting PIN Pad  **In place**  Not i**n place**  Other Secure Cryptographic Device  **In place**  Not i**n place**  **Alternative 2**  **In place.** The solution is listed as P2PE approved solution on [PCI website](https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions),  **In place.** All secure components used in the exterior shield are [listed](https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions) as P2PE components or PTS devices supported by the P2PE solution.  Secure Card Reader  **In place**  **Not in place**  Contactless Secure Card reader  **In place**  Not i**n place**  Encrypting PIN Pad  **In place**  Not i**n place**  Other Secure Cryptographic Device  **In place**  Not i**n place** | **Alternative 1:**  **In place**, I have validated that the product specified in Part 4 is E2EE-validated and exactly the same version can be found on PNC’s list of End-to-End Encryption validated products. Exactly the same version is used in the exterior shield and the following details are exactly the same:   1. Terminal Vendor 2. Manufacturer Name 3. Terminal Model 4. POS Hardware Version 5. Software Version for POS Security Application 6. PED Hardware Version 7. Software Version for PED Security Application 8. PCI PTS Approval number(s) 9. PTS Approval Version 10. Software version for the Payment application 11. Intended Environment 12. PSPs or Member Processors 13. E2EE Validation Date   **Payment Software, Option A:**  **In place**, I have validated that the software version for the Payment application is found on PCI SSC’s list of PA-DSS-validated payment applications and the Reference # for the PA-DSS Validated Payment Application is exactly the same in Part 4 and on the PCI SSC’s list of PA-DSS-validated payment applications.  **Payment Software, Option B:**  **In place**, I have validated that the software version for the Payment application is compliant with PCI Secure Software Standard (SSF Validated Payment Software) and the Reference # for the SSF Validated Payment Software is exactly the same in Part 4 and on the PCI’s list of SSF Validated Payment Software.  I have validated that all secure components used in the exterior shield are listed on [PCI PTS website](https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices):  Secure Card Reader  **In place**  **Not in place**  Contactless Secure Card reader  **In place**  Not i**n place**  Encrypting PIN Pad  **In place**  Not i**n place**  Other Secure Cryptographic Device  **In place**  Not i**n place**  **Alternative 2**  **In place,** I have validated that the solution is listed as P2PE approved solution on [PCI website](https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions).  **In place.** I have validated that all secure components used in the exterior shield are [listed](https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions) as P2PE components or PTS devices supported by the P2PE solution.  Secure Card Reader  **In place**  **Not in place**  Contactless Secure Card reader  **In place**  Not i**n place**  Encrypting PIN Pad  **In place**  Not i**n place**  Other Secure Cryptographic Device  **In place**  Not i**n place** |
| 3 | For each secure component specified in Part 4 of the vendor and product details, the protection against unauthorised replacement, Installation or removal is properly implemented as described in the secure components vendor’s (terminal vendor’s) documentation. | **In place**, implemented according to the document H04. | **In place**, I have verified that it is implemented according to document H04. |
| 4 | The documented routine for daily external inspections exists and includes:   1. pictures of the original exterior shield solution 2. a checklist for detecting modifications to the final version of the exterior shield solution and; 3. A routine on how to act when a modified exterior shield is detected. | **In place** and implemented according to the documented routine for daily external inspections, document H01. | **In place**, I have verified that a documented routine for daily inspections, document H01, has been provided.  **In place**, I have verified that document H01 contains a routine on how to act when a modified exterior shield is detected.  **In place**, I have verified that document H01 contains a checklist with checkboxes and that the document is to be signed and dated as part of the daily inspection.  **In place**, I have verified that a checklist for detecting all known modifications to the final version of the exterior shield solution, document H02 has been provided.  **In place**, I have verified that a clear picture that make it possible to detect any modifications to the final version of the exterior shield solution, document H03 has been provided. |

## Anti-skimming Questionnaire

The Exterior Shield Vendor must complete the Anti-skimming Questionnaire as part of the Exterior Shield review. However, [Best practice: Requirement no. 5 - 11] are only recommendations that are to be considered and do not have to be in place.

| **Best Practice #** | **Requirement** | **Compliance status** | **Vendor description** |
| --- | --- | --- | --- |
| 5 | The exterior shield is equipped with an anti-skimming device that can measure at least one of the following properties:  - Vibrations in the exterior shield  - Electrical measurements of the exterior shield. | In place  Not in place | If in place, state the methods:  Vibrations in the exterior shield  Electrical measurements of the exterior shield.  Additional method, please describe the method used:  Further comments: |
| 6 | The card reader has a mechanism that protects the card from being read by a skimming device when it is inserted into the card reader. Known methods are:  - Jittering of card transport  - Emitting a radio signal that prevents the magnetic stripe to be read before the card is in place. | In place  Not in place | If in place, state the methods:  Jittering of card transport  Emitting a radio signal that prevents the magnetic stripe to be read before the card is in place.  Other method, please describe the method used:  Further comments: |
| 7 | The joint between the card reader and the exterior shield is protected by a sticker with a unique number and an UV-light hologram | In place  Not in place |  |
| 8 | The vendor provides a measure-tool to support the daily check of the exterior shield. | In place  Not in place |  |
| 9 | The recommendations in the [PCI guide Skimming Prevention – Best Practices for Merchants](https://www.pcisecuritystandards.org/documents/Skimming_Prevention_BP_for_Merchants_Sept2014.pdf?agreement=true&time=1560858059474) are followed. | In place  Not in place |  |
| 10 | The exterior shield is alarmed. The watchdog for the exterior shield should be battery-driven in case of loss of power supply. | In place  Not in place |  |
| 11 | The terminal shut down while the exterior shield is open. The watchdog for the exterior shield should be battery-driven in case of loss of power supply. | In place  Not in place |  |

# Vendor Attestation of Compliance

|  | **Vendor Response:** | **Yes** | **No** | **N/A** | **Comment** |
| --- | --- | --- | --- | --- | --- |
| AoC 1 | We, the Exterior Shield Vendor, as identified in Part1, have completed all sections of this document as a self-assessment of the product specified in Part 2 of this document. |  |  |  | Further comments: |
| AoC 2 | We assert the status for each component and each encryption zone identified in Part 2 of this document as **Compliant**: All the requirements are marked as fulfilled (Yes) or not applicable |  |  |  | Further comments: |
| **X** | | | | | |
| **Signature of Executive Officer ↑** | | | | | **Date**: |
| **Name**: | | | | | **Title**: |
| **City:** |

## Third-Party Auditor Attestation of Validation

|  | **Vendor Response:** | **Yes** | **No** | **N/A** | | **Comment** |
| --- | --- | --- | --- | --- | --- | --- |
| AoV 3 | We, the Third-Party Auditor, have: |  |  |  | |  |
|  | 1. assessed Part 1, 2, 3 and 4 of this document (chapter 6.1) |  |  |  | | Further comments: |
|  | 1. verified the Exterior Shield Vendor’s self-assessment of the Exterior Shield specified in chapter 6.2 this document |  |  |  | | Further comments: |
|  | 1. measured the protections angles of the privacy shield specified in chapter 6.2, Best Practice #1 |  |  |  | | Further comments: |
| AoV 4 | We assert the status for the UPT/Exterior Shield as **Compliant**: All the requirements in Report of Validation are marked as fulfilled (Yes) or not applicable |  |  |  | | Further comments: |
| **X** | | | | | | |
| **Signature of Lead Third-Party Auditor Name ↑** | | | | | **Date**: | |
| **Lead Third-Party Auditor Name**: | | | | | **Title**: | |
| **City:** | |

The Form is to be completed and to be signed by both the Exterior Shield Vendor and the Third-Party Auditor. A scanned version of the Form containing chapter 6, with the signatures of both the Exterior Shield Vendor and the Third-Party Auditor including the documentation mentioned in chapter 6.1 Part 3, are to be sent to PNC ([validation (at) pan-nordic.org](mailto:validation@pan-nordic.org)) for validation and subsequent listing in List 5.