

**Self-Checkout Point Vendors
Terminal Vendors
Merchants**

Self-Checkout Points

Best Practice: Self-Checkout Point - Ver C Final

Type: Security
30 October 2018

In brief

In this document the following definitions are used:

Self-Checkout Point – *An attended solution where the customer serves the cashier function and performs the card payment himself.*

Self-Checkout Terminal - *An attended EMV POS terminal connected to a Self-Checkout Point.*

This document presents the PNC SAC Best Practices for fulfilling the brand requirements for Self-Checkout Points. It also presents recommendations for Self-Checkout Points as [Best practice: B: 8-9].

Please note that if the Self-Checkout Point does not fulfil all requirements described in [Best practice: B: 1-7], it will be considered a UPT and will be subject to fulfilling the UPT requirements.

The objective of this document is to present a checklist of requirements for Self-Checkout Points. Please see Appendix A. It shall be used as a checklist for all the above-mentioned stakeholders and the acquirers.

Version history

Date	Version	Description	Issued/revised by
2010-11-25	A Final	A new document	PNC SAC
2017-05-29	B Final	Document review. Updated links and requirement references	PNC SAC
2018-10-30	C Final	Changes in definitions, requirements and recommendations	PNC SAC

1	SCOPE	3
2	MODEL FOR ASSESSING	4
3	REQUIREMENTS	4
4	RISKS AND COUNTERMEASURES	4
5	THE REVIEW PROCESS	5
	APPENDIX A: SELF-ASSESSMENT QUESTIONNAIRE - REQUIREMENTS	6
	APPENDIX A: SELF-ASSESSMENT QUESTIONNAIRE - RECOMMENDATIONS	7
	APPENDIX B: MERCHANT, VENDOR AND PRODUCT DETAILS	8
	APPENDIX B: ATTESTATION OF COMPLIANCE	10
	APPENDIX B: TEMPLATE - SELF-CHECKOUT POINT DESCRIPTION	11
	APPENDIX B: TEMPLATE - EXTERNAL INSPECTIONS	12

1 Scope

This document describes the PNC Best Practices for Self-Checkout Points

It defines the requirements for a security level that acquirers in the pan Nordic market find acceptable.

1.1 Target audience

The main target audience for this document is Merchants. Self-Checkout Point Vendors and Terminal Vendors should also be familiar with the contents of this document.

1.2 Definitions

Self-Checkout Point – An attended solution where the customer serves the cashier function and performs the card payment himself.

Self-Checkout Terminal - An attended EMV POS terminal connected to a Self-Checkout Point.

A POS Terminal for a Self-Checkout Point that does not fully comply with [Best practice: B: 1-7], is regarded as an Unattended Payment Terminal (UPT).

1.3 For more information

If you have any questions regarding this best practice document please contact PNC on e-mail:

- validation (at) pan-nordic.org

1.4 Related Documents

Terminals that cannot release cardholder data (E2EE) – validation status POI (List 1):

<http://www.pan-nordic.org/Renderers/ShowMedia.ashx?id=e5dd07e6-a406-4f2b-bec5-b4be03a96679>

Electronic Cash Registers that do not handle any cardholder data (No cardholder data handling) – validation status ECR (List 2):

<http://www.pan-nordic.org/Renderers/ShowMedia.ashx?id=5f947a99-8dc1-4a06-bf00-6f8fb7f31b4f>

These documents/overviews can be found from PNC website:

<http://www.pan-nordic.org/PanNordicCard/PCI-and-Security/Validated-Products.aspx>

2 Model for assessing

PNC SAC has defined a model for assessing Self-Checkout Points.

The model is based on that:

- The Merchant completes the documentation attached as Appendix A and Appendix B.
- If requested by the acquirer, the Merchant's Self-Checkout Point Vendor sends completed and attested documents, Appendix A and B, to the Acquirer for final approval.

The best practise requirements are defined in the Self-Assessment Questionnaire in Appendix A.

3 Requirements

Self-Checkout Points are to meet the card schemes and acquirer requirements.

A Self-Checkout Point that fulfils the requirements in this document, meets the card schemes requirements for this type of solution. Please note that the generic requirements, such as the PCI and the EMV requirements are not included in this document.

4 Risks and Countermeasures

The main risks connected to Self-Checkout Points are that PIN is noticed together with the card data or the card is stolen. The four main attack scenarios are described below together with proposed countermeasures.

1. **Sniffer device inside the Self-Checkout Point**
 - A sniffer device is used to intercept and to log the traffic from the Self-Checkout Point.
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. A camera is also installed in the PIN 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 is installed on top of the original PIN-keyboard.

General countermeasures

Much fraud can be avoided if:

- The cardholder and the merchant staff are vigilant and have got information on how to distinguish the modified Self-Checkout Point from the original Self-Checkout Point.
- The cardholder is informed to protect the PIN.

To make it easier for the merchant and the cardholder to find modifications, it is recommended that the original solution is presented to the cardholder, for example by presenting a picture of Self-Checkout Point next to the original Self-Checkout Point.

It is also recommended that the cardholder is informed to protect the PIN, for example by covering the PIN-entering with the other hand or with his/her body. This to make sure that a pickpocket cannot see

the PIN.

Countermeasures for Scenario 1

- Make sure that end-to-end encryption validated EMV POS Terminals are used. Alternatively a PCI P2PE listed Solution can be used.

Countermeasures for Scenario 2

- Install the Self-Checkout Point in a way that the cardholder protects the PIN-entering with his/her body.
- Request the cardholder to protect the PIN-entering

Countermeasures for Scenario 3 and 4

- Regular checks

5 The review process

The review process is mainly built on self-assessment. The assessment process is briefly described below.

1. The Merchant provides to the Acquirer the completed:
 - a. Self-Assessment Questionnaire
 - b. required documentation described below
 - c. signed Attestation of Compliance.
2. The Acquirer reviews the complete documentation.

If requested by the acquirer, the Merchant's Self-Checkout Point Vendor completes and attests Appendix A and B and sends them to the Acquirer for final approval together with, at a minimum, the following documentation:

- A documented routine for external inspections
- A description of the Self-Checkout Point

Templates are found in Appendix B.

Appendix A: Self-Assessment Questionnaire - requirements

Best Practice	Requirement	Compliance status	Vendor description
B:1	There must always be a merchant representative present, who is responsible for Self-Checkout Points and who is available upon request and in error situations. The merchant representative must keep Self-Checkout Points under surveillance.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]
B:2	The Self-Checkout Terminal shall not be accessible to cardholders or to the public when the merchant is closed.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]
B:3	The Self-Checkout Point must be placed indoor within the merchant's facilities.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]
B:4	The merchant must perform a check for fraudulent devices at Self-Checkout terminals at least every sixth hour during opening hours, starting with the first check when the merchant opens. The check shall be based on security guidance received from the Terminal Manufacturer and/or Terminal Vendor.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]
B:5	The Self-Checkout Terminal must be locked or in other way attached to the Self-Checkout Point, or alarmed, to avoid theft and unauthorised replacement.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]

Appendix A

B:6	<p>When the cardholder serves the cashier function and performs the card payment himself at a Self-Checkout Point, only purchase transactions are allowed and following functionalities can be supported:</p> <ul style="list-style-type: none"> - Chip - Contactless <p>Following functionalities are not allowed in this mode:</p> <ul style="list-style-type: none"> - Reversal - Signature *) - Magnetic stripe - Referral **) - Key entered card number - Over floor limit in offline mode <p>*) Included BankAxept POS Backup solution **) Included Ringsvar in Sweden</p> <p>This requirement shall be confirmed by your Terminal Vendor.</p>	<input type="checkbox"/> In place When marked in place, it's confirmed by your Terminal Vendor <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]
B:7	Cardholder receipts must be provided in accordance with existing rules for attended terminals.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	[Please provide a short description on how this has been fulfilled.]

Appendix A: Self-Assessment Questionnaire - recommendations

The Self-Checkout Points vendor is also requested to complete the Recommendations Questionnaire. However, [Best practice: B: 8-9] are only recommendations that are to be considered and do not have to be in place.

Best Practice	Requirement	Compliance status	Vendor description
B:8	The Self-Checkout Point may give a visual- and/or audio-signal if attendance is required.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	If in place, comment: [Please provide a short description on how this has been fulfilled.]
B:9	The area where Self-Checkout Points are installed, may be alarmed.	<input type="checkbox"/> In place <input type="checkbox"/> Not in place	If in place, comment: [Please provide a short description on how this has been fulfilled.]

Appendix B: Merchant, Vendor and product details

Part 1: Merchant information

Company Name:			
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:			
Country:		Postcode:	
Organisation/VAT number:		City:	
URL:			

Part 2: Self-Checkout Point Vendor information

Company Name:			
Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:			
Country:		Postcode:	
Organisation/VAT number:		City:	
URL:			

Part 3: Product information for Self-Checkout Point

Model:	
Model - Version:	
Application version Number:	

Part 4: Self-Checkout EMV POS Terminal information

Terminal Vendor name:	
Manufacturer name:	
Model:	
PNC Case ID Alt. P2PE Solution Reference No:	

If an E2EE Validated EMV POS Terminal is used, please use the same name as in the document E2EE Terminal Form.

Appendix B: Attestation of Compliance

This section is to be completed by the Merchant as a declaration of the compliance status with the requirements in SELF-CHECKOUT POINT - VER C FINAL. Complete all the relevant sections and submit to the acquirer.

Based on the results noted in:

- The Self-Assessment Questionnaire, SAQ
- The attached documentation

(Company Name) asserts the following compliance status for the Self-Checkout Point identified under Part 2-4 in Appendix B as

Compliant: All the requirements in SELF-CHECKOUT POINT SAQ are marked in place.

Signature of Merchant Executive Officer ↑	Date:
Executive Officer Name:	Title:

Appendix B: Template - Self-Checkout Point description

Description of the solution

[Instruction:

1. Insert a generic picture showing the Self-Checkout Point, the location of the operator, the location of the Self-Checkout Points and the distances between the Self-Checkout Points and the operator.
2. Insert blueprints or pictures of the Self-Checkout Point and the visual shield.

]

The cardholder dialogue

[Instruction: Provide a description of the displayed cardholder dialogue.]

...

Appendix B: Template - External Inspections

Check that the Self-Checkout Point has not been modified.

The Self-Checkout Point should look as follows:

[Insert picture(s)]

- It is not allowed to install additional equipment, such as rack for folders, on the Self-Checkout Point.
- Check the Self-Checkout Point for holes that can be used for miniature cameras.
- If any modification is spotted shut down the Self-Checkout Point and contact <the support>.
- <The support> contacts the acquiring institution and the police, if needed.