**Self Assessment – No cardholder data handling**

***In brief***

*The assessment on page 2 of this document is applicable for Electronic Cash Register- (ECR), Unattended Payment Terminal- (UPT) and Card Interface- (CI) vendors whose products are integrated against E2EE or P2PE[[1]](#footnote-1) terminals and whose products do not store, process or transmit any account data (cardholder data or sensitive authentication data), except truncated or encrypted account data from the E2EE or P2PE terminal.*

Merchants and acquirers need to know that all installed products are fulfilling the PCI DSS requirements for cardholder data handling. Nordic acquirers are therefore via Pan Nordic Card Association (PNC) running a PCI DSS Compliance programme to ensure that only PCI DSS Compliant products are installed from 1 January 2010 and that all existing installations are meeting the PCI DSS requirements by 1 July 2012.

If the merchant cannot access electronic cardholder data, *the number of applicable PCI DSS requirements is fewer* for the merchant. This is possible to achieve if all of the following is validated: 1) the cardholder data is only handled by an EMV POS terminal that encrypts the cardholder data when the card is read, 2) the cardholder data can only be decrypted by a compliant payment service provider and 3) cardholder data is not handled in any other system than the encrypting EMV POS terminal. These encrypting EMV POS terminals are either:

* End-to-End Encryption-validated EMV POS terminals (E2EE terminals)
* Point to Point Encryption-certified EMV POS terminals (P2PE terminals)

ECR-, UPT- and CI-vendors have two options for making sure that their products comply with PCI DSS:

* **Option 1: ECR-, UPT- and CI-vendors who are integrating their ECRs, UPTs or CIs (Payment Applications) towards** **E2EE or P2PE terminals and are not handling cardholder data**, are requested to use the form in this document to Self Assess their products to provide evidence to merchants and acquirers that:
* The Payment Application does not store, process or transmit any account data (cardholder data or sensitive authentication data), except truncated or encrypted account data from an E2EE or P2PE terminal.
* Cardholder data from previous installations is being removed as part of the installation of the Payment Application
* An Implementation Guide is provided to the merchants to inform the merchant that:
	+ The Payment Application does not store, process or transmit any account data (cardholder data or sensitive authentication data), except truncated or encrypted account data from the E2EE terminal
	+ Any configuration or replacement of the payment application that enables storing, processing or transmitting any account data (cardholder data or sensitive authentication data) will require that the payment application must undergo a full PA-DSS certification performed by an external auditor and all PCI DSS requirements will apply for the merchant validation.
	+ The payment application does not offer manually key-entered transactions via the ECR, UPT or CI. However, it can be offered via the E2EE or P2PE terminal.
* The vendor does not offer a configuration option within the Payment Application, not even via remote update, remote support or for troubleshooting purposes, that enables storing, processing or transmitting account data (cardholder data or sensitive authentication data).
* **Option 2: ECR-, UPT- and CI-vendors who are integrating their ECRs, UPTs or CIs towards other terminals than E2EE or P2PE terminals** usually cannot provide evidence to reduce the number of applicable PCI DSS requirements for their merchants. If the product is handling cardholder data it has to be PA-DSS certified. PA-DSS[[2]](#footnote-2) is a supporting standard to the PCI DSS standard and is used to validate that Payment Applications, such as ECRs, are handling cardholder data according to the PCI DSS standard.

|  |
| --- |
| **Table 1: Receipt guidelines** |
| Cardholder receipts | Online- and offline-authorised transactions  | * Include only the last four digits of the primary account number (PAN), replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as “x”, “\*”, or “#”, and
* Exclude the card expiration date.
 |
| Merchant receipts  | Online-authorised transactions  | * Strongly recommended to include only the last four digits of the primary account number (PAN), replacing all preceding digits with fill characters that are neither blank spaces nor numeric characters, such as “x”, “\*”, or “#”, and
* Exclude the card expiration date.
* Mandatory to include at a maximum the first six and the last four digits of the primary account number (PAN), replacing other digits with fill characters that are neither blank spaces nor numeric characters, such as “x”, “\*”, or “#”
 |
| Offline-authorised transactions[[3]](#footnote-3)  | Any cardholder data except for the data described in the receipts for online transactions must be encrypted. Note that CAV2/CVC2/CVV2/CID, PIN/PIN Block must never be stored, even if encrypted. |

|  |
| --- |
| **Part 1: Vendor Information** |
| Company Name: |       |
| Contact Name: |       | Title: |       |
| Telephone: |       | E-mail: |       |
| Business Address: |       |
| Country: |       | Postcode: |       |
| Organisation number/CVR/VAT number: |       | City: |       |
| URL/Web address: |       |
| **Part 2: Payment Application Information** |
| Product Name: |       |
| Product Version(s)[[4]](#footnote-4): |       |
| **This part is to be completed by the Payment Service Provider before the form is signed** |
| Payment ServiceProvider Company Name: |       |
| Integration(select one alternative) | [ ]  The Payment Application is integrated directly with the E2EE-terminal.[ ]  A separate software module (Card Interface) outside the E2EE-terminal is used. Name:       |
| E2EE- or P2PE-validatedTerminal Model5: |       | E2EE Validation date[[5]](#footnote-5):(Format: yyyy-mm-dd) | 20   -  -   |
| **Intended Environment** |
| EMV: | [ ] Yes[ ]  No | Unattended Payment Terminal (UPT): | [ ]  Yes[ ]  No | Main industry for customers: | Please select main industry for your customers! |
| **Part 3: Self Assessment Questionnaire** |
| The Payment Application in part 2 does not store, process or transmit any account data (cardholder data or sensitive authentication data), except truncated or encrypted account data from the E2EE terminal or the P2PE terminal.  | [ ]  In place |
| The Payment Application vendor in part 1 does not offer a configuration option within the Payment Application in part 2, not even via remote update, remote support or for troubleshooting purposes, that enables storing, processing or transmitting of cleartext account data (cardholder data or sensitive authentication data).  | [ ]  In place |
| The Payment Application does not print or display the complete card number for example on receipts. For details see *Table 1: Receipt Guidelines* on the previous page. | [ ]  In place |
| Cardholder data from previous installations is being removed as part of the installation of the Payment Application. Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the Payment Application, in accordance with industry-accepted standards for secure deletion. | [ ]  In place |
| An Implementation Guide is provided to the merchants to inform the merchant that: 1. The Payment Application in part 2 does not store, process or transmit any account data (cardholder data or sensitive authentication data), except truncated or encrypted account data from the E2EE terminal or from the P2PE terminal
2. Any configuration or replacement of the Payment Application that enables storing, processing or transmitting any account data (cardholder data or sensitive authentication data) will require that the Payment Application must undergo a full PA-DSS certification performed by an external auditor and all PCI DSS requirements will apply for the merchant validation.
3. The Payment Application in part 2 does not offer manually key-entered transactions, except in the E2EE terminal or in the P2PE terminal.
 | [ ]  In place |

The company specified in Part 1of this document asserts the following compliance status for the product and the product versions identified in Part 2 of this document as Compliant: All the requirements in Part 3 of this document are marked in place.

**x**

|  |  |
| --- | --- |
| **Signature of Executive Officer ↑** | **Date**: 202 -  -   |
| **Executive Officer Name**:       | **Title**:       |
| **City:**       |

**Please sign the completed document, scan page 2 and send page 2 per e-mail to the Payment Service Provider who you are working with!**

1. P2PE (Point to Point Encryption) is expected to replace E2EE later on. [↑](#footnote-ref-1)
2. PA-DSS, Payment Application Data Security Standard, <https://www.pcisecuritystandards.org/> [↑](#footnote-ref-2)
3. Please ensure with your Payment Service Provider or your Member Service Provider that it is possible to recreate the transactions. [↑](#footnote-ref-3)
4. **It is strongly recommended that the number of versions is limited and the payment application part of the ECR, the UPT or the CI is handled separately.**

There are two options that cannot be combined available for describing product versions:

	* **Option 1**: If the compliance status does not change between a smaller number of payment applications (PA) more than one version can be self assessed in the same self assessment form, given the following two conditions are met: 1. Only the last digit or letter in the version number is changed. 2. The version numbers are limited both upwards and downwards. Four examples: 3.**1**-3.**3**, 3.2.**1**-3.2.**7**, 3.1.1.00**3**-3.1.1.00**5** and 3.1.1.003.**T**-3.1.1.003.**Z**.
	* **Option 2**: There is also another option. This option cannot be combined with the option described above. This other option means that minor version changes can be described by replacing a digit with an x, where the x means the numbers from 0-9. More than one x can be used to describe the versions. Two examples: 3.**x** means 3.**0**, 3.**1**, 3.**2** etc. up to 3.**9** and 3.**xx**.01.00 means 3.**00**.01.00, 3.**01**.01.00, 3.**02**.01.00 etc. up to 3.**99**.01.00. [↑](#footnote-ref-4)
5. Please see: <http://www.pan-nordic.org/Plugins/ContentEditor/FileStreamer.aspx?path=PNC_files/vendors/PCI%20DSS/Sweden/E2E%20Validation%20Status.pdf> [↑](#footnote-ref-5)