# Vendor and product details – POI

|  |  |  |  |
| --- | --- | --- | --- |
| **Part 1: Terminal vendor information** | | | |
| Company Name: |  | | |
| Contact Name: |  | Title: |  |
| Telephone: |  | E-mail: |  |
| Business Address: |  | | |
| Country: |  | Postcode: |  |
| Organisation number/ VAT number: |  | City: |  |
| Web page/URL: |  | | |

|  |  |
| --- | --- |
| **Part 2: Product information** | |
| Intended product environment: | ECR  Stand-alone |
| The product consists of the following components: | Point of Encryption POI  SAM-card environment with the SAM installed in the Point of Encryption POI |
| **1 - Point of Encryption POI** | |
| Manufacturer name: |  |
| Terminal model: |  |
| Hardware version: |  |
| Software version for Security Application: |  |
| PCI PTS Approval Number(s): |  |
| PCI PTS Approval Version: |  |
| **2 – SAM-card (please fill in the details, if selected above)** | |
| Manufacturer name: |  |
| Device model: |  |
| Hardware version: |  |
| Software version for Security Application: |  |
| **Debit/Credit Application information** | |
| The Debit/Credit application is located in the: | 1 - Point of Encryption POI  2 – SAM-card |
| Software version for Debit/Credit Application: |  |
| PCI SSC’s PA-DSS Reference #: |  |
| **3 - Decryption HOST** | |
| HOST or HOSTs used for the product |  |
| **Protocol Information** |  |
| Terminal to HOST Protocol: |  |
| Terminal to HOST Protocol Version: |  |
| Terminal to ECR Protocol: |  |
| Terminal to ECR Protocol Version: |  |
| **Encryption zones** | |
| Describe the encryption zones and use the reference numbers above: (Complete all the applicable zones.) | The zones,   * Zone 1 – Start point 1 and end point  . The name of the algorithm is       and the key length is      . * Zone 2 - Start point   and end point  . The name of the algorithm is       and the key length is      . |

|  |  |  |  |
| --- | --- | --- | --- |
| **Part 3: Document references** | | | |
| The following references have been used in the self assessment form: | | | |
| **ID** | **Document name** | **Version** | **Date** |
| E01 |  |  |  |
| E02 |  |  |  |
| E03 |  |  |  |
| E04 |  |  |  |
| E05 |  |  |  |
| E06 |  |  |  |
| E07 |  |  |  |
| E08 |  |  |  |
| E09 |  |  |  |
| E10 |  |  |  |

**The Terminal Vendors Self Assessment Questionnaire and the Third Party Report of Validation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security goal** |  | **VISA Data Field Encryption Best Practice Version 1.0** | **The Terminal Vendor Self Assessment Questionnaire (completed by the terminal vendor specified in part 1 of this document) The answers below are applicable for each component and each zone specified in Part 2 of this document.** | **The Third Party Report of Validation (completed by the third party security assessor specified in part 4 of this document). The answers below are applicable for each component and each zone specified in Part 2 of this document.** |
| Limit cleartext availability of cardholder data and sensitive authentication data to the point of encryption and the point of decryption. | DFE1 | Cleartext cardholder data and sensitive authentication data shall only be available at the point of encryption and at the point of decryption. | In place, the application does not transmit plain-text PAN or SAD outside the secure boundaries of the different device(s), and only uses communications methods included in the scope of the PCI-approved POI device evaluation. | In place, I have examined the attached documentation and the POI device(s) application code and have verified that the application(s) does not transmit plain-text PAN or SAD outside the secure boundaries of the different POI device(s), and only uses communications methods included in the scope of the PCI-approved POI device evaluation. It was implemented according to the following documents: E0X. |
| In place, it is not possible to configure the POI device(s) in such way that cardholder data can be accessible in clear outside the secure boundaries of the different device(s). | In place, I have examined the attached documentation and the POI device(s) applications code and have verified that it is not possible to configure the POI device(s) in such way that cardholder data can be accessible in clear outside the secure boundaries of the different device(s). It was implemented according to the following documents: E0X. |
| In place, the POI device(s) cannot receive any cardholder data from any other place than the PED or the card reader. | In place, I have examined the attached documentation and the POI device application code and have verified that the POI device(s) cannot receive any cardholder data from any other place than the PED or the card reader. It was implemented according to the following documents: E0X. |
| DFE2 | All cardholder data and sensitive authentication data shall be encrypted using only ANSI X9 or ISO approved encryption algorithms (e.g. AES, TDES). | In place, all cardholder data and sensitive authentication data is encrypted using only ANSI X9 or ISO approved encryption algorithms (e.g. AES, TDES). | In place, I have verified that all cardholder data and sensitive authentication data is encrypted using only ANSI X9 or ISO approved encryption algorithms (e.g. AES, TDES). It was implemented according to the following documents: E0X. |
| DFE3 | All cardholder data and sensitive authentication data shall be encrypted with the following exceptions:   * The first six digits of the PAN, may be left in the clear for routing purposes in authorization processing. | **Option 1:**  In place, all cardholder data and sensitive authentication data are encrypted.  **Option 2:**  In place, All cardholder data and sensitive authentication data are encrypted with the following exceptions: The first       digits of the PAN are left in the clear for routing purposes in authorization processing. The reason that this is needed for routing purposes is:      . | **Option 1:**  In place, I have examined the attached documentation and have verified that all cardholder data and sensitive authentication data are encrypted. It was implemented according to the following documents: E0X.  **Option 2:**  In place, I have examined the attached documentation and have verified that all cardholder data and sensitive authentication data are encrypted with the following exceptions:  The first       digits of the PAN, are left in the clear for routing purposes in authorization processing. I have also verified with the processor that this is needed for routing purposes. It was implemented according to the following documents: E0X. |
| * The first six and last four digits of the PAN may be displayed by the payment terminal and/or printed on the transaction receipt, in settlement reports, used for selection of account on file, etc. (This does not supersede stricter laws or regulations in place for displays of cardholder data.). | In place, the following information is displayed on: 1. the cardholder receipt[[1]](#footnote-1):  2. the merchant receipt for offline transactions:       3. the merchant receipt for online transactions:       4. the settlement reports:       5. the display texts:       6. any other similar situation:      .  *Please see the receipt guidelines in Table 1 below.* | In place, I have examined the attached documentation and have verified that only the last four digits of the PAN are displayed on the cardholder receipts and that no more than the first six and the last four digits are displayed by the payment terminal in any other case. It was implemented according to the following documents: E0X.    *Please see the receipt guidelines in Table 1 below.* |
|  | DFE4 | Sensitive authentication data must not be stored after authorization even if encrypted (per PCI DSS). | In place, sensitive authentication data is not stored after authorization even if encrypted. | In place, I have verified that sensitive authentication data is not stored and securely deleted after authorization even if encrypted. It was implemented according to the following documents: E0X. |
| In place, store and forward does not contain any other track 2 data than PAN and expire date. The transaction data is encrypted and is only retained until such time as it can be submitted for clearing/settlement, after which, it is deleted.  Not applicable (the terminal is for onboard sale only) | In place, store and forward does not contain any other track 2 data than PAN and expire date. The transaction data is encrypted and is only retained until such time as it can be submitted for clearing/settlement, after which, it is deleted. It was implemented according to the following documents: E0X.  Not applicable (the terminal is for onboard sale only) |
| In place, the clearing transactions do not contain full track 2 data. The clearing transaction data is encrypted. | In place, I have examined the attached documentation and have verified that: 1. the clearing transactions do not contain full track 2 data.  2. the clearing transaction data is encrypted. It was all implemented according to the following documents: E0X. |
| Use robust key management solutions consistent with international and/or regional standards. | DFE5 | Keys shall be managed per ANSI X9.24 (all parts) /ISO 11568 (all parts) or its equivalent within Secure Cryptographic Devices (SCD) such as a PED, HSM, etc., as defined in ANSI X9.97 (all parts) /ISO 13491 (all parts) or its equivalent. | In place, keys are managed per ANSI X9.24 (all parts) /ISO 11568 (all parts) or its equivalent within Secure Cryptographic Devices (SCD) such as a PED, HSM, etc., as defined in ANS X9.97 (all parts) /ISO 13491 (all parts) or its equivalent. | In place, I have verified by review of technical documentation that the keys are managed per ISO 11568 (all parts) /ANSI X9.24 (all parts) or equivalent. It was implemented according to the following documents: E0X. |
| DFE6 | All keys and key components shall be generated using an approved random or pseudo-random process such as NIST SP 800-22. | In place, implemented according to the following documents: E0X. | In place, I have confirmed that keys and key components are generated using a random or pseudo-random process as follows:  1. interviewed responsible personnel and examined documentation to determine:  a. the origin of cryptographic keys  b. the process for generating cryptographic keys.  2. ensured that the device used for key generation is one of the following:  a. the PTS certified device which will use the generated key  b. a PTS certified or FIPS140-2 level 3 certified device.  3. examined cryptogram files (or samples of check values) to validate unique symmetric keys (random/pseudo-random generation).  4. verified that the technical staff have sort on the cryptograms field (or the check digit field or fingerprint field) to make it easier to spot duplicates.  5. checked cryptograms against the manufacturer documentation listing of test or default values.  6. examined asymmetric key fingerprints or hash values to validate unique keys. (Examine public keys to verify uniqueness.)  7. examined vendor certification letters or technical documentation to indicate that the equipment has been designed to meet appropriate standards and specifications.  8. ensured that self-developed implementations of a cryptographic pseudo-random number generator have been certified by an independent laboratory. Testing must include testing in accordance to the statistical tests defined in NIST SP 800-22  9. ensured that the operating environment is maintained within the environmental limits of the equipment.  It was implemented according to the following documents: E0X. |
| DFE7 | Documentation describing the set-up and operation of the key management solution must be made available upon request for evaluation purposes. | In place, documentation describing the architecture (including all participating devices in cryptographic protocols), set-up and operation of the key management solution exist and is demonstrably in use for all key management processes. | In place, I have reviewed documentation describing the key management architecture and cryptographic protocols and confirm that it is complete. Implemented according to the following documents: E0X. |
| DFE8 | Keys shall be conveyed or transmitted in a secure manner. *For example, the key distribution method described in X9/TR-34 Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques, Part 1–Using Factoring-Based Public Key Cryptography Unilateral Key Transport (to be published) or equivalent should be used.* | In place, keys are conveyed or transmitted in a secure manner. | In place, I have verified that keys are conveyed or transmitted in a secure manner and that the following services are provided:   1. key separation 2. key substitution prevention 3. key identification 4. key synchronization 5. key integrity 6. key confidentiality 7. key compromise detection   It was implemented according to the following documents: E0X.  *Please see DFE 13.* |
| * If remote key distribution is used, mutual authentication of the sending and receiving devices shall be performed. | In place, when remote key distribution is used, mutual authentication of the sending and receiving devices is performed.  Not applicable, since | In place, I have verified that when remote key distribution is used, mutual authentication of the sending and receiving devices shall be performed. It was implemented according to the following documents: E0X.  Not applicable, since |
| DFE9 | Keys used in the data field encryption process:   * Must be unique per device. | In place, keys used in the data field encryption process are unique per device (security zone). | In place, I have verified that keys used in the data field encryption process are unique per device (security zone). It was implemented according to the following documents: E0X. |
| * Must only be used to encrypt cardholder data and sensitive authentication data and cannot be used for any other purpose. | In place, keys used in the data field encryption process are only used to encrypt cardholder data and sensitive authentication data and cannot be used for any other purpose. | In place, I have verified that the device enforces:  1. If encryption keys were used only for their stated purpose.  2. If keys used for PIN encryption were never used for account data encryption, and vice versa.  3. If encryption or decryption of arbitrary data occurred using any account data encrypting key or key encoding key contained in the device.  4. If account data keys, key encipherment keys, and PIN encryption keys had different values.  5. If account data keys were used only to encrypt CHD and SAD and were not used for any other purpose.  It was implemented according to the following documents: E0X. |
| * Keys used for PIN encryption must never be used for data field encryption (per PCI PIN Security Requirements). | In place, keys used for PIN encryption are never used for data field encryption (per PCI PIN Security Requirements). |
| Use key-lengths and cryptographic algorithms consistent with international and/or regional standards. | DFE10 | Encryption keys shall have strength of at least 112 equivalent bit strength. The following table summarizes equivalent bit strengths for commonly used approved algorithms   |  |  | | --- | --- | | **Algorithm** | **Bit Length** | | TDES | 112[[2]](#footnote-2) | | AES | 128[[3]](#footnote-3) | | RSA | 2048 | | ECC | 224 | | SHA | 224 |   For details on equivalent bit strengths, see ISO TR-14742  *Recommendations on Cryptographic Algorithms and their Use – Technical Report (to be published 2009).* | In place, encryption keys have strength equivalent of at least 112 bit length (TDES). | In place, I have: 1. interviewed responsible personnel to determine which encryption algorithms are used to encrypt account data.  2. verified by review of technical documentation that the transaction originating device has been designed to meet approval standards for data encryption algorithms per ISO or ANSI X9.52 and mode of operation and a padding mechanism per ISO/IEC 10116:2006).  3. verified by review of technical documentation that the transaction originating device uses the appropriate key length for the algorithm in use.  4. interviewed responsible personnel and/or review documentation to determine the following: 4a. the key management approach used, e.g. fixed key, session key, or DUKPT 4b. the crypto-periods used by the implementation.  5. verified the appropriateness of the crypto-period for each key management approach in use.  It was implemented according to the following documents: E0X. |
| DFE11 | Any methods used to produce encrypted text of the same length and data type as the original cleartext shall be evaluated by at least one independent security evaluation organization and subjected to a peer review; such methods shall also be implemented following all guidelines of said evaluation and peer review including any recommendations for associated key management. | In place, any methods used to produce encrypted text of the same length and data type as the original cleartext has been evaluated by at least one independent security evaluation organization and has been subjected to a peer review.  Not applicable, since | In place, I have examined the attached documentation and have evaluated that all methods used to produce encrypted text of the same length and data type as the original cleartext, that they are subjected to a peer review and that all such methods are implemented following all guidelines of said evaluation and peer review including any recommendations for associated key management. It was implemented according to the following documents: E0X.  Not applicable, since |
| Protect devices used to perform cryptographic operations against physical/logical compromises. | DFE12 | Devices used to perform cryptographic operations should undergo independent assessment to ensure that the hardware and software they are using is resilient to attack. | **Option 1:**  In place, the hardware is PTS-validated and listed on the PCI SSC website, PNC SAC-validated and listed on the PNC website and the PED’s software has been reviewed according to the requirement of the Member Service Provider.  **Option 2: Specific alternative for an intermediate secure device:**  In place, the intermediate secure device’s hardware has been independently assessed according to ISO 13491 (all parts) to ensure that the hardware is resilient to attack. The intermediate secure device’s software has been independently reviewed according to the requirement of the Member Service Provider. | **Option 1:**  In place, I have examined that:  1. the hardware is: 1a. PTS-validated and listed on the PCI SSC website 1b. PNC SAC-validated and listed on the PNC website 2. the PED’s software has been reviewed according to the requirement of the Member Service Provider.  It was implemented according to the following documents: E0X.  **Option 2: Specific alternative for an intermediate secure device :**  In place, I have examined that:  1. the intermediate secure device’s hardware has been independently assessed according to ISO 13491 (all parts) to ensure that the hardware is resilient to attack. 2. the intermediate secure device’s software has been independently reviewed according to the requirement of the Member Service Provider.  It was implemented according to the following documents: E0X. |
| DFE13 | Symmetric and private keys shall be protected against physical and logical compromise. Public keys shall be protected from substitution and their integrity and authenticity shall be ensured. | In place, implemented according to the following documents: E00. | In place, I have verified that keys are conveyed or transmitted in a secure manner and that the following services are provided:   1. key separation 2. key substitution prevention 3. key identification 4. key synchronization 5. key integrity 6. key confidentiality 7. key compromise detection   It was implemented according to the following documents: E0X.  *Please see DFE8.* |
| DFE14 | If any cardholder data (e.g. the PAN) is needed after authorization, a single-use or multi-use transaction ID or token should be used instead.   * A single-use transaction ID is preferred.   + Acceptable methods for producing a single-use transaction ID include hashing of the PAN with a transaction-unique salt value, encrypting the PAN with an approved algorithm using a transaction-unique key, or equivalent. The single-use transaction ID can be produced by other methods provided that the resulting reference data is unique per transaction and the original cardholder data (e.g. the PAN) cannot be reproduced.   **NOTE**: Irrespective of whether the transaction ID is a single use or multi-use, if a salt is used, the salt must be kept secret and appropriately protected. Salt should be a minimum length of 32-bits. | In place    Not applicable, since | **Option 1:**  In place, I have validated that: 1. the method for producing a single-use transaction ID include hashing of the PAN with a transaction-unique salt value, encrypting the PAN with an approved algorithm using a transaction-unique key, or equivalent.  2. the salt is kept secret and is appropriately protected. The salt length is 32-bits or longer.  It was implemented according to the following documents: E0X.  **Option 2:**  In place, the method to produce the single-use transaction ID where the resulting reference data is unique per transaction and the original cardholder data (e.g. the PAN) cannot be reproduced.  It was implemented according to the following documents: E0X.  Not applicable, since |
| * A multi-use transaction ID may be used if there is the need to maintain correlation (of the account) across multiple transactions.   + Acceptable methods for producing a multi-use transaction ID include hashing of the cardholder data using a fixed (but unique per merchant) salt value, or equivalent.   **NOTE**: Irrespective of whether the transaction ID is a single use or multi-use, if a salt is used, the salt must be kept secret and appropriately protected. Salt should be a minimum length of 32-bits. | In place  Not applicable, since | In place, I have validated that: 1. the method for producing a multi-use transaction ID include hashing of the cardholder data using a fixed (but unique per merchant) salt value, or equivalent. 2. the salt is kept secret and is appropriately protected. The salt length is 32-bits or longer.  It was implemented according to the following documents: E0X.  Not applicable, since |

|  |  |  |
| --- | --- | --- |
| **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[[4]](#footnote-4) | 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. |

# Attestation of Compliance

The POI vendor must complete all applicable sections of this document as a declaration of the product specified in part 2 of this document validation status with Visa Best Practices Data Field Encryption version 1.0 (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

Based on the results noted in:

* the Terminal Vendor Self Assessment Questionnaire (“the SAQ”)
* the attached documentation specified in Part 3 of this document
* the Third Party Report of Validation

The company specified in Part 1 of this document asserts the following compliance status for each component and each encryption zone identified in Part 2 of this document as **Compliant**: All the requirements in the SAQ are marked in place or not applicable.

**X**

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

# Third Party Attestation of Validation

The third party security assessor must complete all applicable sections of this document as a declaration of the product specified in part 2 of this document validation status with Visa Best Practices Data Field Encryption version 1.0 (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

|  |  |  |  |
| --- | --- | --- | --- |
| **Part 4: Third Party Information** | | | |
| Company Name: |  | | |
| Contact Name: |  | Title: |  |
| Telephone: |  | E-mail: |  |
| Business Address: |  | | |
| Country: |  | Postcode: |  |
| Organisation number: |  | City: |  |
| Web page/ULR: |  | | |

Based on the results noted in the Third Party Report of Validation, the attached documentation specified in Part 3 of this document and the code review, the company specified in Part 4 of this document asserts the following compliance status for each component and each encryption zone identified in Part 2 of this document as **Compliant**: All the requirements in The Third Party Audit Report of Validation are marked in place or not applicable.

**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 POI vendor and the third party security assessor. A scanned version of the form with the signatures of both the POI terminal vendor and the third party assessor are to be provided to PNC SAC.

1. For Visa and MasterCard only the last four digits of the PAN may be displayed on the cardholder receipts. [↑](#footnote-ref-1)
2. For the purposes of these Best Practices, two key TDES (112-bits) should not process more than 1 million transactions. In cases where the number of transactions potentially processed through the system using a single 112-bits TDES key greatly exceeds 1 million, three key TDES (168-bits) or AES should be used. Note that key management schemes that greatly limit the number of transaction processed by a single key, such as Derived Unique Key Per Transaction (DUKPT) can be used to ensure that any individual key is used only a limited number of times. [↑](#footnote-ref-2)
3. The smallest key size usable with AES is 128 bits. This key size is stronger than needed, but if AES is to be used, it is the smallest available. (Longer keys may of course be used if so desired.) [↑](#footnote-ref-3)
4. Please ensure with your Payment Service Provider or your Member Service Provider that it is possible to recreate the transactions. [↑](#footnote-ref-4)