PAN-NORDIC
CARD ASSOCIATION

Terminal vendors
Third party security assessors

VISA BEST PRACTICES - Data Field Encryption Version 1.0 Evaluation

Best Practice: E2ee Evaluation - Ver E Final
Type: Security
21 October 2011

In brief

POS POI Terminal - A general description of any terminal used to perform a card-based payment transaction when a PIN is required to confirm cardholder authentication.

UPT - A POS POI device where the transaction is initiated by the cardholder, and there is no immediate merchant support available. These include terminals such as: Automated fuel dispensers; Kiosks; and Self-service devices – ticketing/vending or car parking terminals.

In order to assist merchants to procure End-to-End Encryption (E2EE) products that reduce their PCI DSS scope, Pan Nordic Card Association (PNC) has decided to allow terminal vendors to validate POI product compliance with (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

Action required
The terminal vendor, who wants to validate product compliance with (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009), is to make sure that the POI solution fulfils the best practice requirements, is both self assessed and third party validated and that the signed reports of the two assessments are provided to PNC.

Version history

Version	Change
A Final	First version
B Final	The Revised version – Third party review added
C Final	New supporting documents - Third Party Audit Report and Third Party Audit Acknowledgement added
D Final	Additional information requested in Part 2: Product Information and examples given in the vendor description fields.
E Final	The Third Party Audit Report and the Third Party Audit Acknowledgement sections have been merged to a special forms section. Special forms are used for UPT POIs. The free text answers have been replaced by statements that are to be verified in place. It has been clarified that all encryption zones in the solution are to be reviewed. All DFE requirements are validated by a third party security assessor.

1 Background

The marketplace has expressed a growing interest in pursuing data field encryption (also known as end-to-end encryption) of card data. Data field encryption protects card information from the swipe to the acquirer processor with no need for the merchant to process or transmit card data in the “clear.” Importantly, data field encryption renders cardholder data useless to criminals in the event of a merchant data breach. The implementation of any data field encryption solution must be done in a strong and secure way to prevent the compromise of card data. With industry standards still in the development phase, that goal can be particularly challenging. In an effort to enhance overall data security in the payment industry and to further the development of data field encryption, Visa has developed (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009) and (Visa Europe Data Field Encryption: Device and Key Management Guidance, Version 1.0 2010) to assist merchants in evaluating the new encryption solutions emerging in the marketplace.

PCI SSC’s answer to the question: Is encrypted cardholder data considered being cardholder data that must be protected in accordance with PCI DSS?

PCI SSC have answered in (Knowledgebase Article #10359 - Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS 2009) that encrypted data may be deemed out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it.

Any technological implementation or vendor solution should be validated to ensure both physical and logical controls are in place in accordance with industry best practices, prohibiting the entity, or malicious users that may gain access to the entity’s environment, from obtaining access to Keys. Furthermore, service providers or vendors that provide encryption solutions to merchants who have administrative access and controls to Keys along with the management of termination points for encryption to process transactions, are required to demonstrate physical and logical controls to protect cryptographic keys in accordance with industry best practices (such as NIST referenced in PCI DSS requirement 3.6), along with full compliance with PCI DSS.

Merchants should ensure their solution providers who provide key management services and/or act as the point of encryption/decryption are in compliance with PCI DSS. Merchants should be aware that encryption solutions most likely do not remove them completely from PCI DSS. Examples of where DSS would still be applicable include usage policies, agreements with service providers that deploy payment solutions, physical protection of payment assets and any legacy data and processes (such as billing, loyalty, marketing databases) within the merchant's environment that may still store, process or transmit clear text cardholder data, as that would remain in scope for PCI DSS.

2 Scope

This document describes the process to evaluate POI product compliance with (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

The target audience for this document is terminal vendors who would like to offer products that are validated against (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

The definitions used in the Self Assessment Questionnaire are from (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

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

- mail (at) pan-nordic.org

3 Different E2EE solutions

At its simplest form, the E2EE solution is a POI terminal that is connected to an ECR system and to a HOST system. The POI terminal cannot pass on any cardholder data or sensitive authentication data in clear text to the ECR system. Any cardholder data or sensitive authentication data is encrypted in the secure area of the POI terminal before it is sent to the host for decryption.

A more complex form of an E2EE solution is a solution where more than one encryption zone is used and cardholder data or sensitive authentication data is decrypted and re-encrypted in a secure device on its way to the decryption HOST.

4 Short description of the evaluation process

This document describes process to evaluate POI product compliance with (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009) for POI products that use one or more encryption zones.

The process is described below.

1. The POI vendor
    a. completes part 1, part 2 and part 4 of the selected form in 1b below and provides it to PNC SAC before the third party assessment is started
    b. initiates a start-up meeting between PNC SAC, the third party security assessor and the POI vendor.
    c. completes
        a. the POI form if the intended product environment is ECR or stand-alone
        b. the UPT form if the intended product environment is UPT
    d. makes sure that the POI solution is both self assessed and third party assessed and that the signed reports[1] of the assessments are provided to PNC.
2. PNC SAC
    a. reviews the information in 1a above and provides the POI vendor with feedback
    b. checks the assessments and lists the product on the PNC website if the self assessment and the third party security assessment provide evidence that the solution fulfils (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

It is recommended that the POI vendor has a close dialogue with PNC SAC during the process to ensure that all DFE requirements in the form section of this document have been interpreted correctly.

5 The third party security assessor

The third party security assessor's role is to assure that the terminal payment application fulfils the requirements in (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009).

The terminal vendor can select its third party security assessor. The selected third party security assessor shall fulfil the following criteria:

- Shall be a company that is independent of and not commercially influenced by the terminal vendor
- Shall have documented experience of the card industry, PCI DSS, PIN key management and POI terminal architecture
- Until 29 February 2012:
    - Shall confirm with ISO27001 or similar, or
    - Shall be a PA-QSA or P2PE PA-QSA listed on the PCI SSC website.
- From 1 March 2012:

[1] The forms section of this document is to be completed and to be signed by both the POI vendor and the third party security assessor. A scanned version of the completed forms pages with the signatures of both the POI terminal vendor and the third party assessor are to be provided to PNC. The signed completed form is above called the signed reports of the assessments.

  - Shall be a PA-QSA or P2PE PA-QSA listed on the PCI SSC website
  - Only reports of validations from PA-QSAs or P2PE PA-QSAs can be added to the list of validated solutions on the PNC website.

6 Required documentation for the third party audit

In addition to completing the POI or UPT forms, providing the documentation that is requested in the forms and ensuring that the assessor audits the product; the terminal vendor shall present at a minimum the following documentation to the third party security assessor:

- A card data flow documentation
  - The document shall give an overview of the internal card data flow of the terminal and the card data flow via any interface. Examples of interfaces are the terminal to host interface, the card reader, the ECR, the printer and the display.
- A key management description
  - This document shall give a detailed description of the key management of the terminal.
- The software code

The documentation shall cover all the DFE requirements. It shall be noted that further documentation might be requested.

7 The third party security assessment

The Third Party Security Assessor is responsible for auditing the compliance with (VISA BEST PRACTICES - Data Field Encryption, Version 1.0 2009) and for reviewing all the DFE requirements.

E2EE Evaluation Form - POI - Ver E Final or E2EE Evaluation Form - UPT - Ver E Final shall:

- Be signed by the third party security assessor and the terminal vendor
- Confirm that all the DFE requirements are in place.

No other reports or forms than the above-mentioned forms are accepted.

The lowest level for validating that a DFE requirement is in place is to reference another third party security assessor's report where the referenced third party security assessor has verified that the DFE requirement for same product and version is in place. The referenced third party assessor shall use either E2EE Evaluation Form - POI - Ver E Final or E2EE Evaluation Form - UPT - Ver E Final to provide the evidence. The evidence is to be attached to the third party security audit report. Please note that PNC SAC shall be contacted before any references are made to any other report.

8 PNC SAC

The Pan-Nordic Card Association Security Advisory Committee (PNC SAC):

- Performs quality assurance reviews of E2EE reports to confirm report consistency and quality
- Lists E2EE-validated solutions on the PNC Website.
- Qualifies and trains the third party security assessors to perform E2EE-reviews.
- Maintains and updates the E2EE evaluation process.

Note that PNC SAC does not approve reports from a validation perspective. The role of the third party security assessors is to document the terminal vendor's E2EE compliance as of the date of the assessment. Additionally, PNC SAC performs quality assurance to assure that the third party security assessors accurately and thoroughly document results of E2EE assessments.

9 Validity

The approvals are valid as long as the PA-DSS and the PCI PED or PCI PTS approvals for the product are valid.

10 Related Documents

"Knowledgebase Article #10359 - Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS."
http://selfservice.talisma.com/article.aspx?article=10359&p=81. October 2009.
http://selfservice.talisma.com/article.aspx?article=10359&p=81 (accessed November 11, 2009).

"VISA BEST PRACTICES - Data Field Encryption, Version 1.0."
http://corporate.visa.com/_media/best-practices.pdf. 5 October 2009.
http://corporate.visa.com/_media/best-practices.pdf (accessed November 11, 2009).

"Visa Europe Data Field Encryption: Device and Key Management Guidance, Version 1.0."
http://www.visapromotions.net/documents/key_management_guidance_v1_3.pdf. March 2010.
http://www.visapromotions.net/documents/key_management_guidance_v1_3.pdf (accessed March 15, 2010).