



delivering comprehensive
payment security experience

End-to-End Encryption Security Requirements

Revision 1.0

May 27, 2010

Table of Contents

1	Overview	3
1.1	Objective.....	3
1.2	Scope	3
2	Related Publications	4
3	Glossary	5
4	Data to be Encrypted During Transmission	7
4.1	Required Cardholder Data Elements	7
4.2	Optional Data Elements.....	9
5	Key Management Requirements	10
6	Encryption Requirements.....	12
7	Physical Security Requirements (PS).....	13
8	Logical Security Requirements (LS).....	15
9	Encryption Monitoring and Management System Requirements (MM).....	17
10	Appendix: End-to-End Encryption Environments.....	18
10.1	Examples of Encryption Environments.....	18
10.2	Merchant Retail Switch	18
10.3	Gateway/Processor Decryption.....	19
10.4	Direct Connect to Acquirer/Processor	20
11	Requirements Index	22

1 Overview

The Secure POS Vendors Alliance commissioned the End-to-End Security work group to provide clear guidelines on the application of encryption technology to payment card data used for retail financial transactions. These guidelines are meant to promote good information security practices and provide merchants with a clear understanding of what POS equipment encryption features should provide to reduce their information security risks related to payment account data; and as a subsequent benefit reduce their burden of compliance with Payment Card Industry Data Security Standards. This document addresses encrypting payment card data in tamper resistant security modules. This document does not address payment account Issuer standards or technologies. It does not address card, cardholder, or account verification and authorization schemes. It does not address transport layer or communications channel security.

1.1 Objective

Create an industry encryption framework of payment account data utilizing the capabilities of SPVA-approved secure hardware systems to adequately secure payment account data information before it enters the application environment. SPVA is targeting an interoperable solution.

1.2 Scope

The scope of end-to-end encryption requirements covers the enabling technologies that secure payment account data from point of encryption to point of decryption. The SPVA defines end-to-end encryption as follows: The transmission of cardholder data in an encrypted form, from its point of presentment, such that it prevents this data from being known in plaintext until the point of decryption. The SPVA recognizes that end-to-end encryption requirements are complex and potentially difficult and costly for our industry to implement. It is therefore our goal to utilize published standards such as those developed for protection of the debit PIN in payment transactions and innovations in symmetric and public key encryption as a foundation to achieve payment account data security on an international scale. By starting with these well understood principles to secure cardholder data, the requirements will be generated with sound concepts in mind that will lead to faster adoption and understanding by the POS industry. This path also prepares the industry for the worthy and achievable goal of interoperability. The end result of this document will be an auditable set of requirements that can be used to validate cardholder data security across the many entities that participate in the transport of payment card data.

2 Related Publications

Unless specified, refer to the most current version of the referenced publications.

Table 1 Related Publications

Reference	Publication
ANSI X9.24	Banking—Retail Financial Services Symmetric Key Management
ANSI X9.52	Triple Data Encryption Algorithm: Modes of Operation
ANSI TR-31	Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
ISO 9564	Personal Identification Number (PIN) Management and Security
ISO 11568	Banking—Key Management (Retail)
ISO 13491	Banking—Secure Cryptographic Devices (Retail)
ISO 7813	Financial Transaction Card Format
	PCI DSS Standards
	PCI PTS (previously PCI PED) Standards
FIPS 140-2 Level 2	FIPS Standard
	PCI PIN Security Standards
	PCI SSC FAQ http://selfservice.talisma.com/?cid=81&c=58&cpc=MSdA03B2lfY15uvLEKtr40R5a5pV2lnCUB4i1Qj2q2g

3 Glossary

Card Authentication Data – Data specifically designed with the purpose to authenticate that the method of presentment is the original issued to the account holder and not an unauthorized clone.

Cardholder name – The name of the account holder of record that is printed or electronically stored on payment cards.

Contactless Payment – Any method relying on short distance radio communications to convey payment account data, such as Near Field Communications (NFC) or Radio-Frequency Identification (RFID).

Customer Name – Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B data element that describes the payment account holder's name.

Data In Process – State of data as it is either an input or output of particular computing logic or storage. SPVA defers to the PCI PA-DSS for the guidelines on protecting data processed by payment applications.

Data In Transmission – State of data as it is communicated between two points of either processing or storage.

Dictionary attack – The entry of a range of possible input values into an encryption system to create a "dictionary" of plaintext and ciphertext pairs across this range. The resultant "dictionary" is then used to correlate captured outputs with the pre-computed ciphertext to allow for the determination of the input plaintext data without access to a decryption function.

Discretionary data – Discretionary data is the data that appears on the magnetic stripe image after the service code. This includes data such as the CVV or CVC (note that this is not the same as the CVV2 or CVC2 values), and other values which may be assigned at the discretion of the card issuer.

It should be noted that some of the discretionary data fields may be available as fields on an integrated circuit card, as well as the magnetic stripe image.

EMV Card – A payment card which supports the standard for [IC cards](#) ("Chip cards") and IC capable [POS](#) terminals and [ATMs](#), for authenticating [credit](#) and [debit card](#) payments.

End-to-End Encryption – Abbreviated: E2E. The transmission of cardholder data in an encrypted form, from its point of presentment, such that it prevents this data from being known in plaintext until the point of decryption.

Expiry Date – Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2 data element four digits in length that describes the Month and Year of the payment card’s expiration.

Magnetic Stripe Card – A card which has a magnetic stripe that carries information, such as a personal identification number or account number.

Method of presentment – Describes how data pertaining to the payment account is introduced into a payment system.

Examples include: magnetic stripe, EMV card, contactless (near field communication), and does not exclude future methods with the same purpose.

Payment Account Data – Information that identifies the account, issuer of the account, the particular account holder, and issuer discretionary data. Generally understood to be the equivalent of the data elements of ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2. The Payment Card Industry (PCI) Data Security Standards further classifies payment account data either as “cardholder data” and “sensitive account data.”

Payment Account number – The account number represented on the method of presentment. Included in the definition of payment account data.

PCI PTS / PCI PED device – A device that has been approved to the PCI PTS or PCI PED standard, 1.x or above. This does not include devices that are “pre-PCI” approved, or devices approved to any other evaluation scheme.

Primary Account Number – Abbreviated: PAN. Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2 data element that describes to the payment account issuer the numbered account responsible for the financial transaction.

Security Code – The three or four digit card validation code, generally printed on the front or back of the physical card and not present in the track data or track data equivalent (for non-magstripe media). Used to validate that the cardholder is in possession of the payment card when purchasing goods online, by phone or by mail.

Service Code – Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2 data element that is 3 digits in length. It describes certain authorization characteristics of the account and is set by the card brand.

Track Data – Data recorded on ISO Track 1, 2, or 3 of a magnetic stripe.

TRSM (Tamper Resistant Security Module) – A physical device designed to inhibit the disclosure of information stored inside the device. A TRSM should resist and detect tampering; penetration of the device will cause immediate erasure of all secrets and cryptographic keys which reside into the device.

4 Data to be Encrypted During Transmission

4.1 Required Cardholder Data Elements

The following elements of payment account data must be encrypted when data is output from the end-to-end encryption system, regardless of method of presentment including Magnetic Stripe, EMV Card, Contactless Card or Manually entered:

- Primary Account Number
- Discretionary Data
- “Security Code” values (e.g., CVC2, CVV2, CID)

An end-to-end encryption system, compliant to these SPVA requirements, must not allow for this data to be stored or transmitted as plaintext outside of a TRSM within the customer presentment environment. To be considered secure in an encrypted format, neither the plaintext nor the encryption key can be determined through the use of a dictionary attack as defined in the Glossary. It is noted that, when combined with the logical security requirements of this standard, this ensures that this data can now be considered out of scope of PCI DSS, as described in the following PCI SSC FAQ article:

<http://selfservice.talisma.com/article.aspx?article=10359&p=81>

Other data including the full magnetic stripe image or equivalent data, may be optionally encrypted by the end-to-end encryption system. However, it should be noted that some elements of this image, such as the service code, expiry date, and customer name may be required in plaintext by applications outside of the scope of the end-to-end encryption system.

Similarly, it may be necessary to allow for some digits of the PAN to be output in plaintext from the encryption system. For compliance to these requirements, no more than the first six digits and the last four digits of the PAN may be output from the system.

Table 2 Magnetic Stripe Data Elements

S1. #	Tag Name	Length	Description	Payment Card Type	Encryption
1	Primary Account Number	Variable up to 19 characters	Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2 data element that describes to the payment account issuer the numbered account responsible for the financial transaction. This data is always returned by the card.	Magnetic Stripe, EMV, Contactless and manually entered	Required
2	Track 1 or 2 Equivalent Data	Variable	Refers to the ISO/IEC 7813 standard magnetic stripe track 1 format B and track 2 data elements.	Magnetic Stripe, EMV and Contactless	Primary Account number and Discretionary Data is Required to be encrypted. Other fields are optional.
3	Track 1 Discretionary Data	Variable	Discretionary part of track 1 format B according to ISO/IEC 7813	Magnetic Stripe, EMV and Contactless	Required
4	Track 2 Discretionary Data	Variable	Discretionary part of track 2 according to ISO/IEC 7813	Magnetic Stripe, EMV and Contactless	Required

4.2 **Optional Data Elements**

Additional data elements suggested to be encrypted in transmission in the electronic payment transaction message: Zip Code, Merchant Identifier, Social Security Number, or full electronic payment message.

5 Key Management Requirements

Key management covers how the keys are:

- Generated using processes such that it is not possible to predict any keys or determine that certain keys are more probable than other keys.
- Distributed in a secure manner.
- Loaded to secure POS or HSM by using dual control or split knowledge in protected ways so as to prevent unauthorized disclosure of any key component.
- Used in a manner that prevents or detects their unauthorized usage
- Administrated in a secure manner with physical security and secure procedural measures.

The following standards have relevant key management techniques and concepts which should be used as a foundation for the key management requirements in this document.

- PCI DSS v1.2 – Cryptographic key management requirements (defined within sections 3.5 and 3.6)
- PCI PIN Security Guidelines 2.0 (Normative Annex A required for any remote key schema) IBE does not require or rely upon RKI Scheme
- ANSI x9.24 part 1 (Part 2 required for any remote key schema)
- ANSI TR 31 Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- ANSI TR 34 Symmetric Key Management Using Asymmetric Technology
- ANSI TR 39 PIN security guidelines
- ISO 11568 Key Management
- NIST SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- ANSI X9.42 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
- ANSI X9.63 Key Agreement and Key Transport Using Elliptic Curve Cryptography
- NIST SP 800-57 Recommendation for Key Management – Part 1: General (Revised)

General Key Management Guidelines:

- All secret symmetric keys and private asymmetric keys are unique to a device except by chance.
- Cryptographic keys are only used for their sole intended purpose.
- Keys associated with stored encrypted data are changed at least once a year.
- Key Exchanges using Discrete Logarithm based Key Exchange protocols (for example Diffie Hellman) MUST perform calculations in a finite field of size no less than $2^{2,048}$ or in an elliptic curve group of size no less than 2^{224} .
- Key Exchanges using other public key algorithms such as RSA must meet the minimum requirements as stated in Section 6.

6 Encryption Requirements

Data Encryption Methods - Advance Encryption Standard (AES), Triple Data Encryption Standard (TDES), RSA ,Elliptic Curve Cryptography (ECC) or Format-preserving Encryption (FPE).

Cryptographic keys must meet the following criteria:

- TDEA : ≥ 112 bits (excludes parity bits); however, new implementations should use greater than 112 bit keys.
- AES : ≥ 128 bits
- RSA : ≥ 2048 bits (refers to the size of the modulus)
- ECC : ≥ 224 bits (refers to the order of the base point)
- CMAC or HMAC with a key-size of at least 128bits.

Format-preserving Encryption algorithm meeting all of the following requirements:

- Has passed cryptographic analysis by a noted independent cryptographer.
- Expert cryptographic review report must be publicly available for peer review
- A method which is publicly available for peer review
- Uses one of the following:
 - An underlying block cipher of TDEA or AES. A keyed based CMAC or HMAC..

Encryption must be performed inside a Host Security Module/TRSM.

Decryption must be performed using keys which are managed as noted below:

- Hardware implementation of the decryption algorithm directly inside the HSM; or,
- Software implementation of the decryption algorithm with encryption keys managed by an HSM installed in a PCI-DSS compliant environment.

7 Physical Security Requirements (PS)

PS 1 Physical Protection of Key and Key Components (TRSM Criteria)

PS 1.1 The cryptographic keys used to encrypt sensitive data at its origin shall be stored inside a TRSM (Tamper Resistant Security Module).

PS 1.2 The cryptographic keys used to decrypt sensitive data at its destination shall be either:

1. Stored inside a TRSM.
2. Protected by encryption keys which are stored inside an HSM installed in a PCI-DSS compliant environment.

PS 1.3 Key components held by key custodians outside of a TRSM are physically and logically protected (using for example a hardware token protected with by a password) so that it cannot be disclosed to anyone else, other than the key custodian.

PS 1.4 The cryptographic device (TRSM) shall comply with the appropriate security criteria, depending on the nature of the TRSM: PCI PTS requirements for devices like POS terminals and magstripe readers, FIPS 140-2 (or PCI HSM) for devices like HSM (Hardware Security Module).

PS 1.5 Documentation shall be provided by the TRSM supplier to prove that the TRSM has been certified against the selected criteria.

PS 2 Physical Protection for TRSM (Secure Area Criteria)

PS 2.1 If the keys are loaded manually in the TRSM it shall be performed in a secure area. Access controls and 24/7 monitoring shall be in place to protect the secure area under the principals of dual control and split knowledge.

PS 2.2 Key loading operations shall be supervised and logged. Recorded data shall be stored for a period of time in line with PCIDSS requirements.

PS 2.3 Documented procedures shall be established and followed to ensure that a stored TRSM is physically protected against the possibility that the TRSM might be stolen, modified in an unauthorized way, and then returned to storage without detection (e.g., locked access).

PS 2.4 If the TRSM is a HSM, the TRSM shall be stored in a secure area with access controls and 24/7 monitoring in place.

PS 3 TRSM Management

PS 3.1 Inventories are created and maintained to log all TRSM which store cryptographic keys.

PS 3.2 If TRSM are used for back-up purposes, all physical security requirements also apply.

8 Logical Security Requirements (LS)

- LS 1 Documented procedures are set to properly and securely manage TRSM storing keys during its lifecycle. Documentation shall include:
- Inspection procedures and controls in order to ensure that the key loading will be performed in a genuine TRSM.
 - Procedure to remove TRSM from Service: when a TRSM is removed for repair, or permanently removed from service (excluding lost or stolen devices); all operational keys are erased from the TRSM.
 - Procedures and processes exist for Key Revocation.
- LS 2 TRSM management procedures are provided to TRSM operators who have a role in the key loading process and overall key management process.
- LS 3 TRSM operators shall be limited to the fewest number necessary for proper key related operations. TRSM operators shall acknowledge that they have understood their role and responsibility.
- LS 4 If the TRSM allows for the decryption of data, the TRSM shall enforce the logical separation of the encryption and decryption operation(s) so that it is not possible to use an instance of the TRSM as a decryption oracle. That is, it must not be possible for data encrypted at point of encryption to be decrypted at any other point except for **the intended point of decryption**.
- LS 5 The TRSM shall implement methods of encryption that ensure that the application of “dictionary” attacks is impossible.
- LS 6 Applications used to provide encryption services at the point of encryption must be protected within the TRSM in which they operate. Applications must be stored within the secure boundary of the approved TRSM, so that any unauthorized modification of an existing application is infeasible. Authorization for the installation and/or modification of encryption applications must be provided through the use of suitable cryptographic controls, with algorithms and key sizes as noted in Encryption Requirements on page 12 of this document.
- LS 7 Only applications which are protected by these controls are permitted to have access to plaintext cardholder data which is in scope of these requirements, as detailed in Data to be Encrypted During Transmission on page 7 of this document of this document. Any cardholder data within the scope of these requirements must not be output from the secure boundary of the TRSM without the full protection of the end-to-end encryption services provided by that TRSM.

LS 8 All applications used to provide decryption services must be used within a PCIDSS secure environment.

9 Encryption Monitoring and Management System Requirements (MM)

Monitoring and Management of terminating systems should adhere to the following requirements:

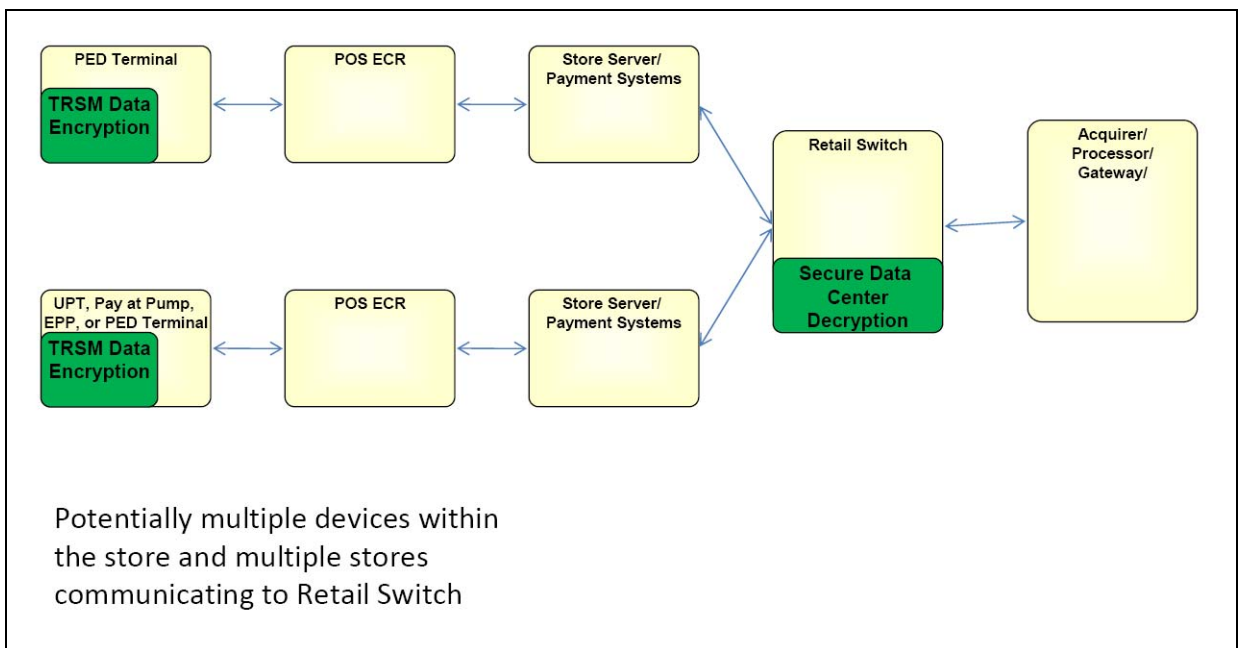
- MM 1 All transactions from encryption-enabled devices generate an auditable log event.
- MM 2 An auditable log event is generated when an unencrypted transaction is received from a device that is registered as a source of encrypted transactions.
- MM 3 An auditable log event is generated when an encryption device is due for a data encryption key change. (Note that PCI DSS requirements dictate a minimum of once per year.)

10 Appendix: End-to-End Encryption Environments

10.1 Examples of Encryption Environments

- Encryption at PED within an integrated environment
- Merchant Retail Switch Decryption
- Gateway or Processor Decryption
- Encryption at PED with direct connect to Acquirer

10.2 Merchant Retail Switch



- **Description**

The data is encrypted at the PED device and decrypted within the retailer's data center.

- **In Scope**

The PED or other TRSM device must adhere to the requirements defined in the SPVA End-to-End Encryption requirements document.

Since the data decryption occurs within the Merchant's data center then this data center must be an approved PCI DSS site.

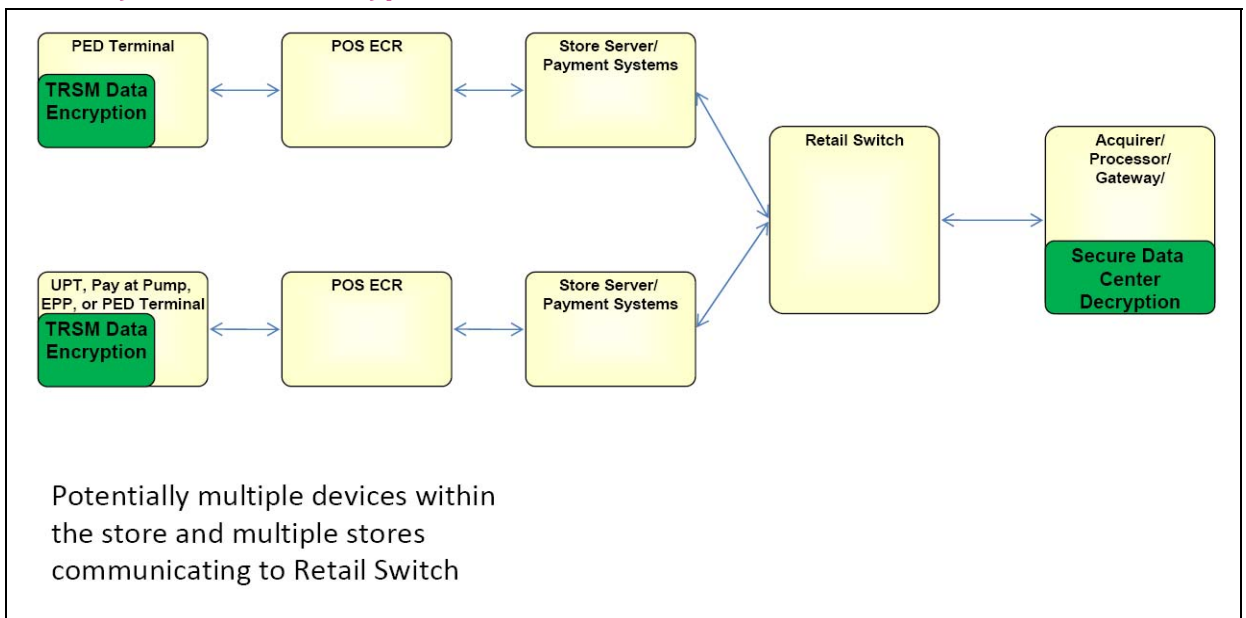
- **Out of Scope**

By following the assumptions below, the POS Terminal (ECR), networks and store server payment systems can be ruled out of scope. These devices and any other device which might be attached to this network must be unable to gather clear card data.

- **Assumptions**

The only ability to decrypt the data is located in the Retailer PCIDSS secured servers. To minimize the scope within the retailer’s environment they must have a properly secured segmented environment with rigorous and strict firewall/router rules.

10.3 Gateway/Processor Decryption



- **Description**

The data is encrypted at the PED device and decrypted at a third party Gateway/Processor.

- **In Scope**

The PED or other TRSM device must adhere to the requirements defined in the SPVA End-to-End Encryption requirements document. It must be confirmed that the merchant has no access to the encryption keys.

Gateway/Processor does decryption and so their data center must be an approved PCI DSS site.

- **Out of Scope**

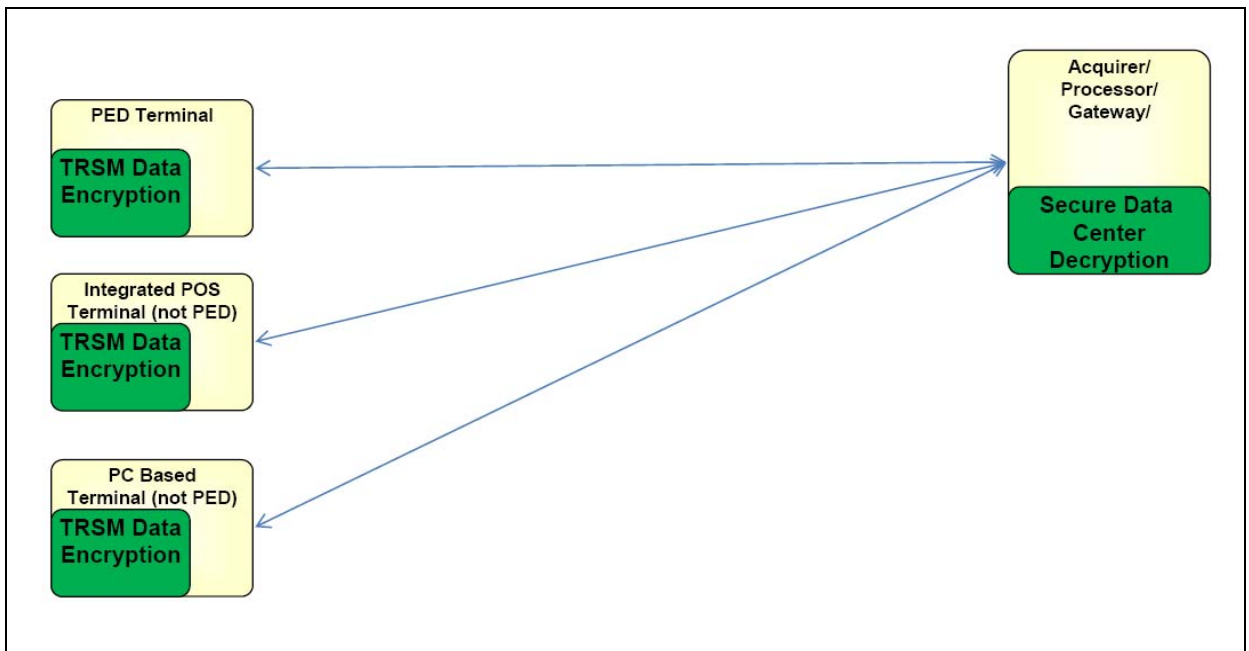
The POS Terminal (ECR), networks, store server payment systems and retail switch are out of scope. These devices and any other device which might be attached to this network must be unable to gather clear card data.

- **Assumptions**

The only ability to decrypt the data is located in the Gateway/Processor PCIDSS secured servers.

The data encryption keys are managed by the Acquirer/Processor and so the merchant has NO access to Decryption Keys and so has no ability to decrypt the card holder data.

10.4 Direct Connect to Acquirer/Processor



- **Description**

The data is encrypted at the PED or other TRSM device and decrypted at a third party Gateway/Processor.

- **In Scope**

The PED or other TRSM device must adhere to the requirements defined in the SPVA End-to-End Encryption requirements document. It must be confirmed that the merchant has no access to the encryption keys.

Gateway/Processor does decryption and so their data center must be an approved PCI DSS site.

- **Out of Scope**

The network from the terminal to the Acquirer/Processor is out of scope. The Payment terminal and any other device which might be attached to this network must be unable to gather clear card data.

- **Assumptions**

The only ability to decrypt the data is located in the Gateway/Processor PCIDSS secured servers.

The data encryption keys are managed by the Acquirer/Processor and so the merchant has NO access to Decryption Keys and so has no ability to decrypt the card holder data.

11 Requirements Index

Physical Security Requirements (PS)

PS 1 Physical Protection of Key and Key Components (TRSM Criteria)

PS 1.1 Encryption key components must be stored in a TRSM.

PS 1.2 Decryption key components must be stored in a TRSM or encrypted.

PS 1.3 Key components held by a custodian must be protected.

PS 1.4 TRSM complies with required security criteria.

PS 1.5 TRSM supplier provides documentation proving compliance.

PS 2 Physical Protection for TRSM (Secure Area Criteria)

PS 2.1 Manual key loading takes place in a secure location.

PS 2.2 Key loading operations shall be supervised and logged.

PS 2.3 TRSM storage is protected.

PS 2.4 HSMs are stored in a secure area with 24-hour monitoring.

PS 3 TRSM Management

PS 3.1 Inventories are created and maintained to log all TRSM storing cryptographic keys.

PS 3.2 If TRSM are used for back-up purposes, all physical security requirements also apply.

Logical Security Requirements (LS)

LS 1 Procedures for securely managing TRSM storing keys are documented.

LS 2 TRSM management procedures are provided to TRSM operators.

LS 3 TRSM operators shall be limited to the fewest number necessary.

LS 4 TRSM cannot be used as a decryption oracle.

LS 5 TRSM ensures that dictionary attacks are impossible.

LS 6 Applications providing encryption must reside within the TRSM.

LS 7 Only applications within scope may have access to plaintext card data.

LS 8 Decryption must be performed in a PCI-DSS secure environment.

Encryption Monitoring and Management System Requirements (MM)

- MM 1** All transactions from encryption-enabled devices generate an auditable log event.
- MM 2** Unencrypted transactions from encrypted devices generate an auditable log event.
- MM 3** An auditable log event is generated when key rotation is due.