VOLTAGE SECUREDATA PAYMENTS FOR PCI P2PE V2

TIM WINSTON | PA-QSA (P2PE), CTGA, CISSP, CISA

COALFIRE®

North America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

OVERVIEW

Voltage engaged Coalfire Systems, Inc. (Coalfire), a Payment Card Industry (PCI) Point-to-Point-Encryption (P2PE) Qualified Security Assessor Company (QSAC), to conduct an independent technical and compliance assessment of Voltage SecureData Payments for use in PCI P2PE Solutions. Coalfire conducted technical testing, an architectural assessment, and a compliance baselining relative to the PCI P2PE standard.

Coalfire describes how the usage of Voltage SecureData Payments can address PCI P2PE requirements as part of a PCI P2PE Solution, including:

- Domain 1 Encryption Environment
- Domain 2 Terminal Payment Applications
- Domain 5 Decryption Environment
- Domain 6 Encryption Key Management

AUDIENCE

This assessment report has three target audiences:

1. **Encryption Solution Providers:** This audience has, or is planning, an encryption solution for card present payments, with encryption immediately on capture by software on a secure payment terminal. For PCI P2PE a secure payment terminal is defined as a PCI Pin Transaction Security (PTS) listed point of interaction (POI), with the Secure Reading and Encryption of Data (SRED) option. Voltage SecureData provides encryption and tokenization for payment and other sensitive information. Voltage SecureData Payments can be used to implement PCI P2PE solutions, if configured and implemented to meet the PCI P2PE standard that can be validated and listed on the PCI website.
2. **P2PE Qualified Security Assessors P2PE (QSAs)**: Assessing a P2PE solution requires detailed technical understanding of solutions to ensure that both technical requirements and process requirements are met. This paper is intended to provide the information needed to assess P2PE solutions that use Voltage SecureData Payments.
3. **Merchants**: Merchants considering P2PE merchant-managed solutions can use P2PE Decryption Environment component providers or other third party key management service providers to implement their solution. PCI P2PE v2.0 does not permit merchants to operate their own hybrid decryption solutions (where the decryption server has clear data decryption keys). Merchant operated solutions may also complete a Non-listed Encryption Solution Assessment (NESA) to demonstrate to their acquires that they have appropriate controls that limit their DSS compliance scope.

ABOUT VOLTAGE SECUREDATA PAYMENTS

Voltage SecureData Payments is intended to increase the security of card-present payments without impacting the buyer’s experience. Encryption solutions based on Voltage SecureData Payments reduce merchant risk of compromised credit card data and potentially reduce the number PCI DSS controls applicable to the retail payment environment substantially.

Voltage SecureData Payments implements encryption of sensitive credit card data in point-of-interaction (POI) devices' firmware, immediately on swipe, insertion, tap, or manual entry. Sensitive card information can only be decrypted by a PCI DSS solution provider, PCI P2PE solution provider, or PCI P2PE Decryption component provider, typically a payment service. Even a compromise of the Point-of-Sale (POS) workstation connected to the POI device would not expose customer's sensitive data.

Voltage SecureData Payments may be successfully configured in a P2PE Hybrid solution implementation. Merchants who wish to develop and maintaining their own encryption solution will not be able to qualify for a PCI P2PE merchant-managed solution, due to the exclusion of hybrid implementations from merchant-managed solutions. According to PCI *P2PE: Solution Requirements and Testing Procedures, v2.0 (Rev 1.1)* Domain 4 Applicability and Eligibility:

> *If a merchant outsources the decryption environment to a PCI-listed P2PE decryption-management component provider, Domain 4 would not apply for the merchant-managed solution, and use of a PCI-listed component provider would be noted in the merchant-as-a-solution-provider's P2PE Report on Validation (P-ROV). If a merchant outsources the decryption environment to a non-listed decryption service provider, Domain 4 would also not apply and Domain 5 (covering the outsourced decryption services) would be assessed as part of the merchant-as-solution provider's P2PE assessment and included in the merchant's P-ROV.*
>
> Therefore, *merchants acting as their own solution provider must meet the following additional criteria to be eligible for P2PE solution validation:*
>
> - Only use hardware-based decryption as part of the P2PE solution (use of hybrid decryption in a merchant-managed P2PE solution is not permitted).

Merchants deploying Voltage SecureData Payments as part of a merchant-managed solution will need to use a third-party service provider to operate the SecureData Payments decryption environment in order to be eligible as a PCI P2PE merchant-managed-solution. Merchants who wish to manage their own decryption environment using Voltage SecureData Payments may still reduce the PCI DSS controls applicable to their point of sale systems and networks, as we will discuss below.

ABOUT THE PCI P2PE PROGRAM

The Payment Card Industry Data Security Standard (PCI DSS) is a critical part of preventing credit card compromise and fraud, but maintaining compliance to PCI DSS can be a complex process for merchants. Depending on how they process credit card account data, a merchant may be required to meet up to 251 PCI DSS security requirements, validated through as many as 1,218 tests.

Encryption is an important part of the PCI DSS standard and protecting card data. Within PCI DSS there are requirements for key management and encryption of card data when it is stored (Requirement 3), and when it is transmitted via wireless (Requirement 2) or untrusted networks (Requirement 4). There is no requirement to encrypt card data when it is transmitted via physical medium within the cardholder data environment (CDE), which is one reason why all systems within the CDE must be held to the highest level of security to help prevent eavesdropping on these unencrypted communications. Even when encryption is used to protect data in transit from host to host, cardholder data is still unencrypted in the application layer of each host, making it vulnerable to memory scraping malware—the source of numerous data breaches in recent years.

In 2011, the PCI Security Standards Council (PCI SSC) launched the P2PE Program to standardize protections for encryption that can simplify compliance for merchants. Transactions protected through P2PE are encrypted within the point of interaction device (POI), and all sensitive data elements remain encrypted until they are safely transmitted to a secure location for decryption and processing (e.g., the gateway or processor). The P2PE program does not replace PCI DSS, but offers eligible merchants an effective option for removing certain network assets from scope, and reducing the number of applicable controls for the remaining environment. This reduction of applicable controls may result in as few as 24 PCI DSS requirements, as assessed on the Self-Assessment Questionnaire P2PE (SAQ P2PE), or on the merchant's Report on Compliance.

PCI SSC issued a major revision to the P2PE standard in 2015, P2PE v2. While the required controls received modest revisions, they were re-organized to better fit how the services are commonly provided. and to introduce P2PE Components Providers. Component Providers offer services that are validated against defined subsets:

COMPONENT	DESCRIPTION
Encryption Management	Provide services for lifecycle management of POI devices
Decryption Management	Provide decryption services
Key-Injection Facility	Provide direct or remote key injection into POI devices
Certification Authority/Registration Authority	Provide data authentication services for keys and other data (e.g. firmware updates) using asymmetric key standards, typically Public Key Infrastructure (PKI).

Component Providers are listed on the PCI website and may be used by P2PE solution providers.

Another major change to P2PE v2 was the addition of P2PE merchant-managed-solutions (MMS). With MMS, a merchant can validate their own P2PE solution and receive the DSS scope benefits of using a P2PE solution. P2PE MMS require strict separation of duties between the decryption environment and Encryption Environment. This is commonly met by merchants using a listed Decryption Component Provider, which ensures that individuals with access to decryption keys are managed by a separate organization.

ABOUT THE NON-LISTED ENCRYPTION SOLUTION ASSESSMENT (NESA)

Since its introduction in 2011, the P2PE standard has been criticized for being too difficult to attain, and for failing to provide compliance guidance for entities that use encryption outside of the defined constraints of this program, due to business requirements, legacy device usage, or other limitations.

In November 2016, the PCI SSC released an information supplement entitled Assessment Guidance for Non-Listed Encryption Solutions[1]. This document outlines a recommended approach for performing an

[1] PCI SSC. (2016). Information Supplement: Assessment Guidance for Non-Listed Encryption Solutions

assessment, called a NESA, of secure encryption solutions that do not fully meet PCI P2PE requirements, to provide their merchants with actionable steps towards assessing the compliance of their environments.

How It Works

While the process for assessing a non-listed solution may be somewhat involved, the principles outlined in this guidance are straightforward:

1. The solution provider should be actively looking to achieve full P2PE compliance, or be fully compliant but providing support to legacy devices that fail to meet program requirements.
2. The decryption environment and key management practices (including key strength, key injection, and/or remote key injection) must be fully-compliant with Domain 5 and Domain 6.
3. The POI devices must be PTS-approved to 2.x or above, although features such as Secure Reading and Encryption of Data (SRED) and Open Protocols are optional.

Assuming these criteria are met, a QSA (P2PE) may conduct a review of the full solution, documenting its compliance with the P2PE standard for each of the six domains. Where the assessed entity does not meet requirements to Domains 1, 2, 3, or 4, the assessor will identify compliance deficiencies and make recommendations for additional PCI DSS security controls to offset or directly address these deficiencies (e.g., additional physical controls or inspections to offset the lack of SRED tamper responsive functionality).

Upon completion of the assessment, the QSA (P2PE) will provide the solution provider with NESA Summary Documentation, which the solution provider would then provide to its merchants, enterprises, other service providers at its discretion (the Summary Documentation is not made available from PCI's website). This document follows a template and instructions provided by PCI for this purpose, ensuring consistent formatting and actionable guidance for merchants and their QSA.

For more information on both P2PE and NESA, please see *Point-to-Point Encryption Opportunities and Challenges for Solution Providers*, Coalfire, 2017[2].

BENEFITS TO MERCHANTS FOR USING PCI P2PE AND NON-LISTED ENCRYPTION SOLUTIONS

The PCI P2PE program provides an official sanctioned path to scope reduction for systems and environments that only have access to P2PE-encrypted data and no access to decryption keys. As a result, such systems have no feasible access to the underlying cardholder data, and thus can be considered outside the cardholder data environment. For people, processes and technologies that remain in the environment, the number of PCI DSS control requirements that apply is drastically reduced, from 251 to only 24 controls[3]. Merchants using P2PE Solutions can therefore realize substantial cost and time benefits from these reduced compliance requirements.

PUBLIC CLOUD PLATFORMS FOR PCI P2PE

There are obvious benefits of implementing encryption solutions and key management on secure public cloud platforms, like Microsoft Azure, Amazon AWS, or IBM Bluemix. SecureData's scalable design and dynamic key management is particularly well suited to cloud deployment. With respect to point-to-point encryption (P2PE) for payment authorization, service providers may use public cloud implementations for their P2PE solution offerings and maintain their PCI – DSS compliance. Those service providers, interested in validating their PCI P2PE implementation, should consider that any environment that handles PCI data

[2] Coalfire Systems (2017). https://www.coalfire.com/Solutions/Audit-and-Assessment/PCI/Point-to-Point-Encryption

[3] PCI SSC. (2017). PCI DSS v3.2 Self-Assessment Questionnaire SAQ P2PE

or encryption keys must be assessed by its P2PE QSA. Cloud providers generally do not support audits for individual customers. Therefore, it is recommended that service providers consider a hybrid public-private cloud approach. For example, VMware on AWS or Azure Stack could provide support for HSMs and other hardware specifically configured for PCI P2PE compliance. Use of a private cloud to implement decryption and key management while leveraging the connectivity, scalability, dynamic networking, and management automation of public clouds, could achieve the desired flexibility and satisfy PCI P2PE requirements.

SUMMARY FINDINGS

FINDINGS

Voltage SecureData Payments clears two of the highest hurdles for implementing P2PE solutions:

1. **Implementation of compliant encryption key management.** PCI P2PE key management requires split knowledge and dual control for every key management function – generation, transmitting, loading, storage, and deletion – for each type of key. Typical, manual processes require development of compliant process, consistent training of all employees involved, and detailed record keeping of all operations. Secure rooms are specified for carrying out these manual processes. Voltage SecureData automates or eliminates almost all manual key management process. Only Hardware Security Module (HSM) Master Keys are created and backed up using manual processes. All other encryption keys for the solution are automatically managed by Voltage SecureData. While offset somewhat, by requirements necessary to support Voltage SecureData Payment's hybrid decryption model (5D-1.12, 5D-1.13, 5D-1.14, 6F-2.1.5, 6H), this can still represent a **30-50%** savings in implementation of P2PE compliant key management[4].

2. **Use of Voltage Identity-Based Encryption (IBE) for POI device keying.** Traditionally, keys are inserted in POI by manually connecting each device to a special key loading device in a secure facility – an expensive step in the terminal supply chain. This also makes it difficult to change terminal keys and requires a second organization to manage sensitive encryption keys. Voltage SecureData Payments enrolls and authenticates terminals during the deployment process using IBE, without requiring a secure key loading room or a manual process for each device, and without trusting another organization. Customers are not limited to acquiring terminals from supported facilities, as with traditional key injection systems. Terminal enrollment at installation, enabled by Voltage IBE, is faster and offers more flexibility for merchants. It is also substantially faster to implement as part of a P2PE Solution because it eliminates the need to establish relationships with KIFs and manual processes for secure exchange of encryption keys – eliminating the risk of key exchange and expense of development and validation of key transmission and loading processes. This eliminates the 1-2 month process of establishing a relationship with each supported KIF from the time of implementing a P2PE solution.

The following are highlights of Coalfire's technical and compliance evaluation of Voltage SecureData Payments for implementing PCI P2PE solutions.

Domain	Overview	Impact
Domain 1: Encryption Device and Application Management	The secure management of the PCI-approved POI devices and the resident software.	Minimum Impact: Select POI that can support Voltage SecureData Payments Terminal SDK in SRED

[4] Based on Coalfire analysis of effort implementing key management and hybrid decryption controls.

Domain	Overview	Impact
Domain 2: Application Security	The secure development of payment applications designed to have access to clear-text account data intended solely for installation on PCI-approved POI devices.	High Impact: Voltage SecureData Payments Terminal SDK meets all requirements for encryption, key management, coding, and processes.
Domain 3: P2PE Solution Management	Overall management of the P2PE solution by the solution provider, including third-party relationships, incident response, and the P2PE Instruction Manual (PIM).	Minimum impact: P2PE Instruction Manual (PIM) simplified by IBE enrollment of POI
Domain 4: Merchant-Managed Solutions	Separate duties and functions between merchant encryption and decryption environments.	No impact: MMS must use Decryption Component Provider or key management service provider
Domain 5: Decryption Environment	The secure management of the environment that receives encrypted account data and decrypts it.	High Impact: Voltage SecureData Payments Appliance and Host SDK enable meeting hybrid decryption requirements for key management, decryption, access control, logging, and monitoring.
Domain 6: P2PE Cryptographic Key Operations and Device Management	Establish and administer key-management operations for account-data encryption POI devices and decryption HSMs.	Maximum Impact: Eliminates the virtually all manual key management processes. Since Derived Unique Key Per Transaction (DUKPTT is not used, there are no Base Derivation Keys (BDK) to share with KIFs, or Key Encryption Keys (KEK) for exchanging BDK. These are replaced by built-in key rotation and key provisioning to POI with IBE

Voltage SecureData Payments can be implemented to meet PCI P2PE requirements as follows:

Encryption Environment (Domain 1) – POI devices are available for solutions that can implement applications using Voltage SecureData Payments Terminal SDK using PTS SRED functions for encryption, key storage, and random number generation. Solution providers must be careful to select POI that have either implemented the Voltage SecureData Payments Terminal SDK in SRED firmware or have P2PE Payment Applications that meet Domain 2 requirements. Reach out to Voltage technical support or your local sales rep for the current list of payment partners and supported terminals.

POI Payment Application (Domain 2) – Voltage SecureData Payments Terminal SDK allows the use of built-in encryption, key storage, and random number functions. Transaction encryption, key storage, and random number functions must be part of the terminal's PTS SRED testing for the POI to be eligible for inclusion in PCI P2PE solutions. Because the Voltage SecureData Payments Terminal SDK is supplied as source code, it is available for the source code reviews and forensic testing required by P2PE Domain 2. A PA-QSA (P2PE) must assess each specific application's use of the Voltage SecureData Payments Terminal SDK. The Voltage SecureData Payments Terminal SDK is developed, tested, and maintained in accordance to all P2PE Domain 2 requirements.

Decryption Environment (Domain 5) – Voltage SecureData Payments requires validation of a hybrid solution (as opposed to a hardware solution where transaction decryption is exclusively performed by an HSM). Data decryption takes place on the server where the Voltage SecureData Payments Host SDK is installed. Data decryption keys are cached in memory and, optionally, in encrypted files on this server. PCI P2PE requirements for hybrid architecture are described in *PCI P2PE: Solution Requirements and Testing Procedures, v2.0 (Rev 1.1)* requirements 5D and 6H. These requirements include stringent technical, physical, and logical access controls and other measures to protect systems that have data decryption keys. Network and system implementation must take these requirements into account when planning a P2PE solution. At a minimum, the decryption environment must include the HSM, Voltage SecureData Key Server, and the server using the Voltage SecureData Payments Host SDK for transaction decryption. Voltage SecureData Payments authentication, authorizations, and logging can, and must, be configured to meet relevant requirements. Voltage SecureData Payments and Voltage SecureData Payments Host SDK provide extensive logging to enable solution providers to meet monitoring and alerting requirements for hybrid P2PE solutions.

Key Management (Domain 6, also applies to Domains 1 and 5) – Two HSM models are supported, both of which are FIPS 140-2 Level 3 compliant: Atalla HSM and Thales nShield. Voltage SecureData Payments uses symmetric encryption (AES FPE FF1) for transaction data encryption and asymmetric encryption for encryption key distribution (ISO/IEC 18033-5 and IEEE 1363.3). Key lengths that comply with Domain 6 Annex C can be configured. Voltage SecureData Payments protocols meet P2PE requirements for protecting keys during storage and transmission. Because Voltage SecureData automates most key management functions and eliminates the need to inject initial keys in POI, it simplifies or eliminates key management processes compared to typical P2PE solutions.

PCI P2PE reference documents:

- https://www.pcisecuritystandards.org/documents/P2PE_v2_r1-1.pdf
- https://www.pcisecuritystandards.org/documents/P2PE_v2_Glossary.pdf
- https://www.pcisecuritystandards.org/documents/P2PE_Program_Guide_v2.0.pdf

MEETING PCI P2PE REQUIREMENTS USING VOLTAGE SECUREDATA PAYMENTS

VOLTAGE SECUREDATA PAYMENTS IMPLEMENTATION FOR PCI P2PE V2.0

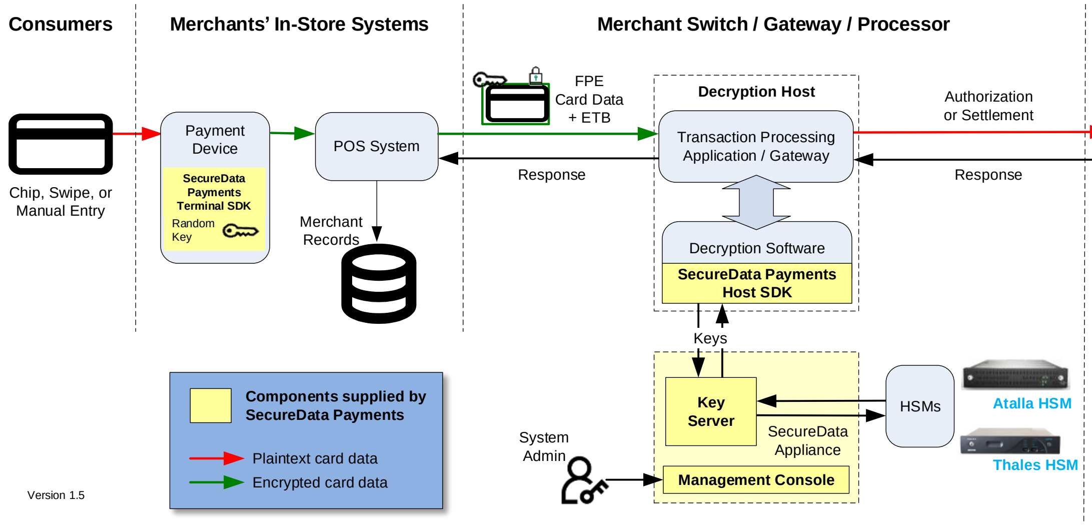
Consumers
Merchants' In-Store Systems
Merchant Switch / Gateway / Processor
Card Networks and Issuers
Chip, Swipe, or Manual Entry
Payment Device
SecureData Payments Terminal SDK
Random Key
POS System
Merchant Records
FPE Card Data + ETB
Response
Decryption Host
Transaction Processing Application / Gateway
Decryption Software
SecureData Payments Host SDK
Authorization or Settlement
Response
Keys
Key Server
SecureData Appliance
HSMs
Atalla HSM
Thales HSM
System Admin
Management Console
Components supplied by SecureData Payments
Plaintext card data
Encrypted card data
Version 1.5

Figure 1: Voltage SecureData Payments Components

Voltage SecureData Payments has three components:

1. Voltage SecureData Appliances manage private keys for data decryption and connects to hardware security modules (HSM) for the highest security private key storage and key management.
2. Voltage SecureData Payments Terminal SDK is a library that may be compiled into an encryption solution's Point of Interaction (POI) terminal application or POI firmware.
3. Voltage SecureData Payments Host SDK is a library that provides decryption and key management services with the Voltage SecureData Appliance.

The Key Matrix (PCI P2PE Report On Validation Table 6.1) for Voltage SecureData Payments is as follows:

KEY TYPE	DESCRIPTION	PURPOSE	CREATION METHOD	DISTRIBUTION	PROTECTED BY	DESTRUCTION
HSM Master Key	256 bit AES	Protect all other keys in the solution	By HSM during commissioning	Only in HSM and backup smartcards	HSM and smartcard quorum	Zero-ize HSM / Physical destruction of smartcards
Master Secret	256 bit random	Per district, per algorithm. Used to derive other key types	By HSM automatically created by Key Manager whenever a new District is created	Stored in Key Manager and data backup	HSM Master Key	Delete or replace in Key Manager / Delete backup

KEY TYPE	DESCRIPTION	PURPOSE	CREATION METHOD	DISTRIBUTION	PROTECTED BY	DESTRUCTION
IBE key	BB1 / 3072 bit RSA equivalent strength asymmetric key pair	Encrypt ETB from terminal	Private key is derived from Master Secret, Time Value, and Identity String by Key Manager (using HSM) / Public key is calculated by terminals using Public Parameter Block (Note: Public Parameters must be signed, or use a comparable method, for distribution to POI to ensure integrity)	Derived when needed. Cached in Key Manager volatile memory	HSM Master Key	N/A. Not stored.
FPE key	128 bit AES FFX mode	Encrypt sensitive transaction data	POI SRED random function	From POI to decryption host / SRED key store on POI / Host SDK key cache on decryption host	IBE public key / cache file key on decryption host	SRED key replacement or deletion on POI / Host SDK secure key deletion
Voltage SecureData Encrypted File Storage key	128 bit AES	Encrypt FPE keys stored on decryption host	Derived from Master Secret by Key Manager (using HSM)	Derived when needed to read cache file	Master Secret	N/A. Not stored.

Cryptoperiods for keys can be configured by solution providers as described in the following table:

KEY TYPE	CRYPTOPERIOD	MECHANISM	DISCUSSION
HSM Master Key	Manual process	Disable HSM on the Voltage SecureData Payments Management Console. Create new HSM Master Key per vendor instructions. Enable HSM on the Voltage SecureData Payments Management Console. Create a new District to create a new set of Master Secrets protected by the new HSM Master Key. Use of previously existing Districts must be discontinued.	It is common practice, although not advised, to use HSM Master Keys indefinitely. This is contrary to NIST SP800-57 Part 1 Rev 4 which recommends a 3-year cryptoperiod. This can be longer if a risk rationale exists. However, lack of a defined cryptoperiod and rotation procedure likely indicates that the key compromise procedures are incomplete or untested.

KEY TYPE	CRYPTOPERIOD	MECHANISM	DISCUSSION
Master Secret	Manual process	Create a new District. Distribute Public Parameters to POI.	Creating a new District creates new Master Secrets for each key type. The Public Parameter Blocks enable the POI to calculate new IBE public keys for the new District. The original District continues to function until deleted, so distribution to POI can be phased. Districts can also be used to segregate different customers or services. A District used for a PCI P2PE Solution must not be shared with other services.
IBE key	Automated daily and manual. 1 day minimum cryptoperiod	The year, month, and day used as the identity date when generating the associated ETB which includes the FPE key. The rotation is configurable by the solution provider. IBE keys can also be rotated manually by creating a new District and distributing a new Public Parameters to each POI.	The automatic use of time periods to change the IBE public key is sufficient to protect against brute force attacks on the private key from over-exposure of the public key. However, a procedure for manual rotation using a new District should be defined and tested to support key compromise procedures.
FPE key	Automated,configurable	New FPE keys can be as frequent as every transaction, although this would impact the performance of the POI and the decryption host.	Typical implementations perform key rollover periods are once-per-day or once-per-week. A new FPE is generated on each POI boot. New random, symmetric keys can also be initiated by events, such as POI power cycle or processing a defined number of transactions.
Voltage SecureData Encrypted File Storage key	Automated, configurable, and manual	Use the reserved Key Rotation Group “StorageEncryption” to configure rotation of all persistent Host SDK data.	Beginning with version 4.1, the Host SDK provides a new implementation of encrypted file-based caching, known as Encrypted File Storage. Encrypted File Storage encrypts all sensitive data, such as cryptographic keys and POI authentication data, cached in files by your Host SDK application using an identity-based encryption key managed by your Voltage SecureData Key Server. Expired ETB and other data should be purged from memory and file caches.

Voltage SecureData Payments is distinguished from other encryption mechanisms by two enabling technologies:

1. With Format-Preserving Encryption (FPE), credit card numbers and other types of structured information are protected by retaining the data format or structure. In addition, data properties are maintained, such as the Luhn checksum and field separators. Portions of the data can remain in the clear. This aids in preserving existing processes such as BIN routing or use of the last four

digits of the card in customer service scenarios. FPE FF1 is a mode of AES encryption, as described by the NIST SP800-38G standard, and accepted by the PCI SSC as strong encryption.

2. Identity-Based Encryption (IBE) eliminates the complexity of traditional Public Key Infrastructure (PKI) systems and symmetric key systems. In other words, no digital certificates or keys are required to be injected or synchronized with payment terminals. Voltage uses IBE to enable end-to-end encryption from capture-to-processor and swipe-to-trusted-merchant applications. IBE is an ISO (ISO/IEC 18033-5) and IEEE (IEEE 1363.3) standard for asymmetric encryption key management.

As a result, Voltage SecureData Payments is a secure, versatile, and scalable encryption solution for card-present and MOTO payments.

For an implementation that uses all the components shown in Figure 1, the boundary of the P2PE decryption environment would be as shown in Figure 2.

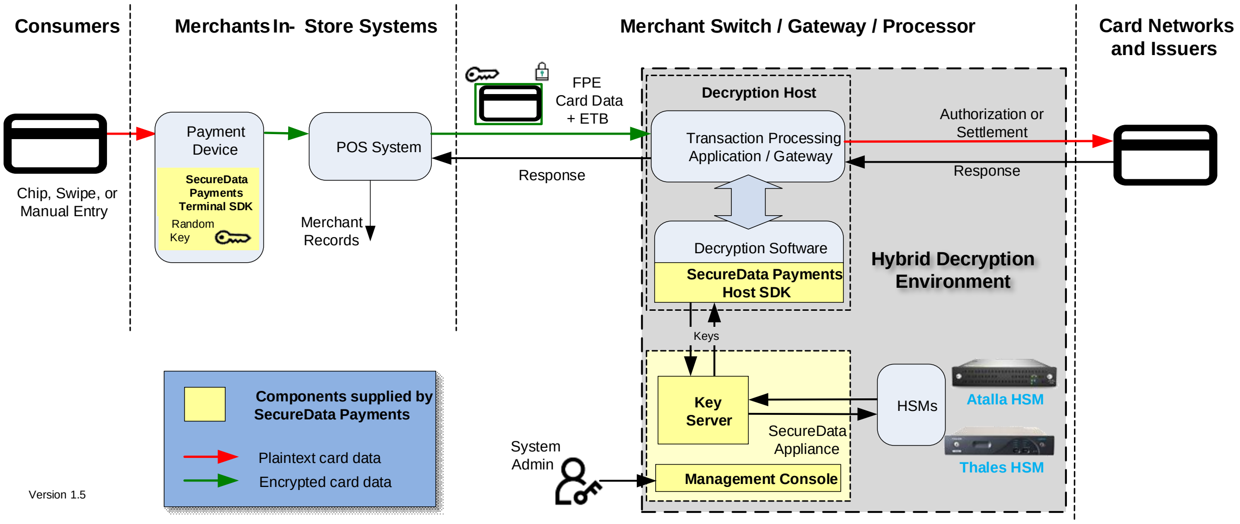
Consumers
Merchants In- Store Systems
Merchant Switch / Gateway / Processor
Card Networks and Issuers
Chip, Swipe, or Manual Entry
Payment Device
SecureData Payments Terminal SDK
Random Key
POS System
Merchant Records
FPE Card Data + ETB
Response
Decryption Host
Transaction Processing Application / Gateway
Authorization or Settlement
Response
Decryption Software
SecureData Payments Host SDK
Hybrid Decryption Environment
Keys
Key Server
SecureData Appliance
HSMs
Atalla HSM
Thales HSM
Management Console
System Admin
Components supplied by SecureData Payments
Plaintext card data
Encrypted card data
Version 1.5

Figure 2: P2PE Decryption Environment

RELEVANT PCI P2PE REQUIREMENTS

Coalfire identified all P2PE v2.0 requirements that are impacted using Voltage SecureData Payments. Each requirement was assessed as to how Voltage SecureData Payments meets the requirement and any configurations or implementation considerations.

For identified requirements, Voltage SecureData Payments has one or more impacts:

- **Meets Requirement**: Voltage SecureData Payments technology or process conforms to the requirement. The Solution, Component, or Application Provider technology or process will also need to meet the requirement. The solution, application, or component provider needs to implement Voltage SecureData Payments per the instructions under “Applicability” to be compliant.
- **Supports Requirement**: Voltage SecureData Payments features enables solution, component, or application providers to meet the requirement.
- **Minimizes Requirement**: The applicability of the requirement is substantially reduced for solutions or components implemented using Voltage SecureData Payments.
- **No Impact**: Voltage SecureData Payments does not impact the requirement. These are included to clarify requirements that appear to apply to Voltage SecureData Payments process or technology.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
Domain 1		
1A-1.1 *Encryption operations must be performed using a POI device approved per the PCI PTS program (e.g., a PCI-approved PED or SCR), with SRED (secure reading and exchange of data).*	Meets Requirement	Voltage SecureData Payments relies on AES FPE FF1 format preserving encryption and key generation implemented as part of a terminal’s SRED functionality. Solution providers need to verify from vendors that these functions are part of the SRED-tested firmware for any POI supported by a solution. Terminals are available that have included Voltage SecureData Payments Terminal SDK in their SRED firmware.
1C-1.2 *Processes for any whitelisting functionality must include:* • *Implementing whitelisting functionality in accordance with the device vendor's security guidance or the application’s Implementation Guide.* • *Cryptographic signing (or similar) prior to installation on the POI device by authorized personnel using dual control.* • *Cryptographic authentication by the POI device’s firmware* • *Review of whitelist functionality to confirm it only outputs non-PCI payment brand account/card data.*	No Impact	Voltage SecureData Payments Terminal SDK does not provide any whitelisting or BIN exclusion functionality.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
• *Approval of functionality by authorized personnel prior to implementation* • *Documentation for all new installations or updates to whitelist functionality that includes the following:* – *Description and justification for the functionality* – *The identity of the authorized person who approved the new installation or updated functionality prior to release* *Confirmation that it was reviewed prior to release to only output non-PCI payment brand account/card data*		
Domain 2		
2A-2.2, 2A-2.3, 2A-2.4 *The application must not store PAN and/or SAD (even if encrypted) as follows:* • *Application must not store PAN data after the payment transaction is complete.* • *Application must not store SAD after authorization is complete.*	Meets Requirement	Voltage SecureData Payments Terminal SDK does not store PAN or SAD data. It is held in volatile memory until encrypted data is produced, then securely deleted.
2A-3.4 *Any whitelisting functionality implemented by the application must include guidance in the application's Implementation Guide…*	No Impact	Voltage SecureData Payments Terminal SDK does not implement any whitelisting functionality.
2B-1.1 *Applications must be developed based on industry best practices and in accordance with the POI device vendor's security guidance, and information security is incorporated throughout the software development life cycle.*	Meets Requirement	Voltage SecureData Payments Terminal SDK development processes meet all PCI P2PE Domain 2 requirements.
2B-1.4.2 *Application risk-assessment techniques (e.g., (application threat-modeling) must be used to identify potential application-security design flaws and vulnerabilities during the software-development process.*	Meets Requirement	Voltage SecureData Payments Terminal SDK undergoes risk-assessment as a regular part of its development process.
2B-3.1.1 *The application developer must provide key-management security guidance describing how cryptographic keys and certificates have to be used.*	Meets Requirement	Voltage SecureData key use is described in the *Voltage SecureData Architecture Guide*. Terminals are provided with a signed parameter block used to derive the solution provider's public key (3072 bit RSA equivalent) using IBE. The integrity of this public key is assured by the integrity controls on the parameter block and derivation process. The SRED key generation function of the terminal is used to generate a 128 bit AES symmetric key for encrypting transaction data. This key is stored in the terminal's SRED key storage. The symmetric key is protected by the public key for transmission to the solution provider.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
2B-4.1 *The application must not encrypt clear-text account data. This means the application must not implement any encryption functions that bypass or are intended to be used instead of the approved SRED functions of the POI device.*	Supports Requirement	Applications need to ensure that encryption SRED functions are used for account data. This can be implemented either by using a POI that has Voltage SecureData Payments Terminal SDK implemented as part of its SRED functionality or by defining AES and random number generator (RNG) alternate implementations (per *Voltage SecureData Payments Terminal SDK Developer Guide,* Annex A) to use terminal SRED functions.
2C-1.1 *Software developers must establish and implement a process to identify and test their applications for security vulnerabilities and implementation errors prior to every release (including updates or patches) using manual or automated vulnerability assessment processes.*	Meets Requirement	Voltage SecureData Payments Terminal SDK development processes meet all PCI P2PE Domain 2 requirements. It is tested for vulnerabilities with both manual and automated processes.
2C-1.2 *Software vendors must establish and implement a process to develop and deploy critical security updates to address discovered security vulnerabilities in a timely manner.*	Meets Requirement	Application developers are notified of all Voltage SecureData Payments Terminal SDK updates and discovered vulnerabilities.
2C-3 *The process to develop, maintain, and disseminate an Implementation Guide for the application's installation, maintenance, upgrades and general use...*	Meets Requirement	Complete implementer documentation for Voltage SecureData Payments Terminal SDK is provided and revised with each release.
Domain 5		
5A-1.1 *All hardware security modules (HSMs) must be either:* • *FIPS140-2 Level 3 (overall) or higher certified, or* • *PCI PTS HSM approved.*	Meets Requirement	Voltage SecureData Payments supports either the Atalla HSM or Thales nShield HSM. Both are FIPS 140-2 Level 3 certified.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5A-1.1.2.b *If the HSM is operated in non-FIPS mode or non-FIPS validated software has been added to the HSM, review the solution provider's written confirmation and confirm that it includes the following:* - *Description of why the HSM is operated in non-FIPS mode* - *Purpose and description of any non-FIPs validated software added to the HSM* - *A statement that nothing has been changed on, or added to, the HSM that impacts the security of the HSM, cryptographic key-management processes, or P2PE requirements.*	Meets Requirement	The HSM is operated in non-FIPS mode and non-FIPS validated software has been added. 1. The HSM operates in non-FIPS mode, after completing a FIPS-mode boot and integrity validation. This is to allow support for IEEE 1363.3 and ISO 18033-5 accepted standard method for IBE key derivation. 2. The software added to the HSM implements the BB1 IBE extraction algorithm as specified in ISO 18033-5 and IEEE 1363.3. 3. IEEE 1363.3 and ISO 18033-5 IBE Key public-private derivation methods are supported natively by Atalla HSM's and as an execution extension in Thales HSM's provided by Micro Focus. The HSM's FIPS validated software and hardware is not modified in this process.
5B-1.1 *Current documentation must be maintained that describes or illustrates the configuration of the decryption environment, including the flow of data and interconnectivity between incoming transaction data from POI devices, all systems within the decryption environment, and any outbound connections.*	Meets Requirement	Documentation provides descriptions of transaction and key flows for Voltage SecureData Payments in the Voltage SecureData Architecture Guide. It is important to note that the Voltage SecureData Appliance never stores or processes unencrypted keys. All keys are protected by the HSM master key. Data decryption keys (DDK) are obtained from the HSM by the Voltage SecureData Payments Host SDK, but are never present in the Appliance.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5B-1.2 *Procedures must be implemented to provide secure administration of decryption devices by authorized personnel, including but not limited to:* • *Assigning administrative roles and responsibilities only to specific, authorized personnel* • *Management of user interface* • *Password/smart card management* • *Console and non-console administration* • *Access to physical keys* • *Use of HSM commands.*	Supports Requirement	Administrative roles and responsibilities be defined for all systems in the decryption environment, including the HSM, Voltage SecureData Appliance, and decryption server running the Voltage SecureData Payments Host SDK. The Voltage SecureData Appliance, including the Console and Command Line Interface, provide authentication and permission management that can be configured to meet P2PE standards. In particular, commands which manage creation of new keys or key rotation must be configured to use dual control. Administration of the decryption server depends on the operating systems and software used. Access controls, remote access, and administration must be implemented to meet the 5B-1.2 requirements.
5B-1.3 *Only authorized users/processes have the ability to make function calls to the HSM—e.g., via the HSM's application program interfaces (APIs).*	Supports Requirement	Follow instructions in Voltage SecureData Atalla HSM Supplement or Voltage SecureData Thales HSM Supplement, as appropriate, to establish communications with the HSM. Additionally, network controls should be used to prevent connections to the HSM from any unauthorized systems.
5B-1.4 *POI devices must be authenticated upon connection to the decryption environment and upon request by the solution provider.*	Meets Requirement	Terminal authentication was introduced in version 4.2 of the Voltage SecureData Payments Terminal SDK, as described in the Voltage SecureData Payments Terminal SDK Developer Guide. Terminals must be enrolled, as instructed, before they can process encrypted transactions. Implementers can either use this optional feature or implement their own authentication method by extending the Voltage SecureData Payments Terminal SDK.
5B-1.7 *Processes are implemented to ensure that clear-text account data is never sent back to the encryption environment.*	Supports Requirement	Voltage SecureData Payments Terminal SDK does not provide any mechanism to return clear-text (or other data) to the terminal.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5B-1.8 *Any truncated PANs sent back to the encryption environment must adhere to the allowable number of digits as specified in PCI DSS and/or related FAQs that specify allowable digits.*	Meets Requirement	Voltage SecureData Payments Terminal SDK FPE functions preserve the first six and last four characters of the PAN, compliant to PCI requirements.
5B-1.9 *Any whitelisting functionality implemented in the decryption environment that transmits data to the encryption environment must ensure that the ONLY allowed output of clear-text account data is for non-PCI payment brand account/card data…*	No Impact	Voltage SecureData Payments Terminal SDK does not provide whitelisting support. The payment application that calls the Voltage SecureData Payments Terminal SDK may offer whitelisting or BIN exclusion.
5C-1.2 *Mechanisms must be implemented to detect and respond to suspicious activity, including but not limited to:* • *Physical breach* • *Tampered, missing, or substituted devices* • *Unauthorized logical alterations (e.g., configurations, access controls)* • *Unauthorized use of sensitive functions (e.g., key-management functions)* • *Disconnect/reconnect of devices* • *Failure of any device security control* • *Encryption/decryption failures* • *Unauthorized use of the HSM API*	Supports Requirement	Voltage SecureData Appliance and Voltage SecureData Payments Host SDK log all errors and events including failed access attempts, account use, key management activities, configuration changes, encryption error, and other relevant functions. Logs may be used for detecting suspicious activities and demonstrating PCI P2PE compliance. Solution providers are responsible for implementing Voltage SecureData Payments Host SDK logging callbacks, as described in *Voltage SecureData Payments Host SDK Developer Guide,* to ensure that all required events and errors are logged. Logging callbacks were introduced in version 4.2.
5C-1.3 *Mechanisms must be implemented to detect encryption failures, including at least the following:* • *Checking for incoming clear-text account data.* • *Detecting and reviewing any cryptographic errors reported by the HSM* • *Detecting and reviewing any unexpected transaction data received.* • *Reviewing data sent by any POI devices that are causing an unusually high rate of transaction authorization rejections.*	Supports Requirement	Any encryption errors cause the associated logging callback function to be invoked. Solution providers are responsible for implementing Voltage SecureData Payments Host SDK logging callbacks, as described in the *Voltage SecureData Payments Host SDK Developer Guide*, to ensure that all required events and errors are logged.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5C-1.4 *All suspicious activity must be identified and a record maintained, to include at least the following:* - *Identification of affected device(s), including make, model, and serial number* - *Identification of affected merchant, including specific sites/locations if applicable* - *Date/time of incident* - *Duration of device downtime* - *Details of whether any account data was transmitted from the POI device during any identified time that encryption was malfunctioning or disabled*	Supports Requirement	Voltage SecureData Payments Host SDK logging can support detection and logging of suspicious activities. Solution providers are responsible for implementing Voltage SecureData Payments Host SDK logging callbacks, as described in the *Voltage SecureData Payments Host SDK Developer Guide*, to ensure that all required events and errors are logged.
5D-1.1 *The solution provider must maintain current documentation that describes, or illustrates, the configuration of the Host System, including the flow of data and interconnectivity between all systems within the decryption environment.*	Meets Requirement	Documentation provides guidance for software, system, and network in the *Voltage SecureData Architecture Guide* and the *Voltage SecureData Appliance Installation Guide*.
5D-1.4 *All application software installed on the Host System must be authorized and have a business justification.*	Meets Requirement	Voltage SecureData Payments Host SDK must be installed on a host system to decrypt transactions from enrolled terminals. This system, or systems, are referred to at the Host System in this document and is subject to all 5D controls that refer to Host System. The Voltage SecureData Appliance or Key Server also has a clear-text data decryption key in transcient memory when HSM calls are proxied between the Host System and HSM. This means that the Appliance or Key Server is subject to all 5D controls that refer to Host System.
5D-1.6 *The Host System must perform a self-test when it is powered up to ensure its integrity before use. The self-test must include:* - *Testing integrity of cryptographic functions.* - *Testing integrity of firmware.* - *Testing integrity of any security functions critical to the secure operation of the Host System.*	Meets Requirement	Voltage *SecureData Payments Host SDK Developer Guide* describes how self-tests of cryptographic functions are performed when a HostContext is created, beginning with version 4.2. Solution providers are responsible for other integrity tests of the Host System. Voltage SecureData Appliance performs self-tests of cryptographic functions, firmware, and all security functions on start up.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5D-1.7 *The Host System must perform a self-test when a security-impacting function or operation is modified (e.g., an integrity check of the software/firmware must be performed upon loading of a software/firmware update).*	Meets Requirement	Voltage SecureData Payments Host SDK must be restarted whenever updated. With the Host instantiation, a new HostContext is created that triggers the self-test execution. Solution providers are responsible for other integrity tests of the Host System. Voltage SecureData Appliance performs self-tests of cryptographic functions, firmware, and all security functions on start up or update.
5D-1.8 *The Host System must enter an error state and generate an alert upon any of the following events:* • *Failure of a cryptographic operation* • *Failure of a system self-test, as described in Requirements 5D-1.6 and 5D-1.7* • *Failure of a security function or mechanism*	Meets Requirement	Voltage SecureData Payments Host SDK calls the associated callback function for all errors. The solution provider is responsible for implementing error responses. Voltage SecureData Appliance enters an error state and must be restarted on failure of self-tests or security functions. The Voltage SecureData Appliance does not perform cryptographic operations.
5D-1.9 *Alerts generated from the Host System must be documented and result in notification to authorized personnel and initiate a response procedure.*	Supports Requirement	Voltage SecureData Payments Host SDK calls the associated callback function for all errors. The solution provider is responsible for implementing error responses. Voltage SecureData Appliance logs all errors. The solution provider is responsible for implementing error responses.
5D-1.10 *The Host System must not perform any cryptographic operations under any of the following conditions:* • *While in an error state, as described in Requirement 5D-1.8* • *During self-tests, as described in Requirements 5D-1.6 and 5D-1.7* • *During diagnostics of cryptographic operations.*	Supports Requirement	Voltage SecureData Payments Host SDK calls the associated callback function for all errors. The solution provider is responsible for implementing error responses. Voltage SecureData Appliance enters an error state and must be restarted on failure of self-tests or security functions. The Voltage SecureData Appliance does not perform cryptographic operations.
5D-1.11 *All source code and executable code for cryptographic software and firmware on the Host System must be protected from unauthorized disclosure and unauthorized modification.*	Supports Requirement	The solution provider is responsible for implementing system integrity protection on the Host System. Voltage SecureData Appliance implements system integrity protection.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5D-1.12 *The clear-text data-decryption keys must not be accessible to any processes or functions not directly required for decryption operations.*	Meets Requirement	Voltage SecureData Payments Host SDK caches clear-text decryption keys in memory, which is protected by operating system process controls. Clear-text decryption keys may optionally be cached in Voltage SecureData Encrypting File System files, as described in the Voltage *SecureData Payments Host SDK Developer Guide.* Voltage SecureData Appliance does not provide any access to clear-text data-decryption keys.
5D-1.13 *The clear-text data-decryption keys must only be accessible to authorized personnel with a defined job-related need to access the keys.*	Meets Requirement	Voltage SecureData Payments Host SDK does not provide access to clear-text keys for access to calling applications or individuals. Personnel with root or administrator access could circumvent operating system protections by accessing page files or core dumps. Solution providers are responsible for controlling system administrator access. Voltage SecureData Appliance are not accessible, except to root system users with forensic or systems tools.
5D-1.14 *The Host System must not write clear-text cryptographic keys to persistent storage (e.g., hard drives, removable storage, flash drives etc.) except for the following:* • *Memory 'swap/page' file purposes.* • *'Core dumps' of memory required for troubleshooting.*	Meets Requirement	When file caching is configured decryption, keys are written to files within a Voltage SecureData Encrypted File Storage (EFS) volume which encrypts all content before storing on disk or other media. EFS encryption keys are managed by Voltage SecureData Key Server. This ensures that only encryption keys ultimately protected by the HSM master key are written to persistent storage. Voltage SecureData Appliance does not write clear-text keys to persistent storage.
5D-2.1 *Host user passwords must be changed at least every 30 days.*	Supports Requirement	Voltage SecureData Management Console authentication can be configured to use local accounts or a central LDAP service. Either can be configured for 30-day password expiration. Note that the Voltage SecureData Appliance is a Decryption Host referred to in the requirement. The Voltage SecureData Management Console must be configured to meet this requirement. Solution providers are responsible for configuring all host system, application account, and Voltage SecureData Console parameters.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5D-2.2 *User passwords must meet the following:* • *Consist of eight characters in length,* • *Consist of a combination of numeric, alphabetic, and special characters, or* • *Have equivalent strength/complexity.*	Supports Requirement	Voltage SecureData Management Console authentication can be configured to use local accounts or a central LDAP service. Either can be configured for the required password parameters. Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
5D-2.4 *User accounts must be locked out of the Host System after not more than five failed attempts.*	Supports Requirement	Voltage SecureData Management Console authentication can be configured to use local accounts or a central LDAP service. Either can be configured for lock out after more than 5 attempts. Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
5D-2.5 *The Host System must enforce role-based access control to include, at a minimum, the following roles:* • *Host System operator role – for day-to-day non-sensitive operations of the Host System.* • *Host System administrator role – configuration of host OS, security controls, software and user accounts.* • *Cryptographic administrator role – configuration of cryptographic management functions* • *Host System security role – auditing of host functions*	Supports Requirement	Voltage SecureData Appliance can be configured for system and Console administrator roles, per the *Voltage SecureData Appliance Installation Guide.* Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
5D-2.6 *The segregation of duties must be enforced between roles, through automated or manual processes, to ensure that no one person is able to control end-to-end processes; or be in a position to compromise the security of the Host System.*	Supports Requirement	Voltage SecureData Appliance can be configured for system and Console administrator roles, per the *Voltage SecureData Appliance Installation Guide.* Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
5D-2.7 *Changes to a Host System user's account access privileges must be managed:* • *Using a formal change-control procedure.* • *Requiring the participation of at least two persons. Therefore, the party making the change cannot authorize the change on their own.* • *Ensuring all changes to access privileges result in an audit log.*	Supports Requirement	Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
5D-3.1 *All non-console access to the Host System must use strong cryptography and security protocols.*	Supports Requirement	Voltage SecureData Console can implement strong cryptography as described in the *Voltage SecureData Appliance Installation Guide.* Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
5D-4.1 *The Host System must be located within a physically secure room that is dedicated to decryption operations and transaction processing.*	Supports Requirement	Solution providers are responsible for configuring all host system, and application account, and Voltage SecureData Console parameters.
Domain 6		
6A-1.1 *Examine documented key-management policies and procedures to verify that all cryptographic keys use algorithms and key sizes that are in accordance with Normative Annex C: Minimum and Equivalent Key Sizes and Strengths for Approved Algorithms.*	Meets Requirement	Voltage SecureData Payments encrypts transaction data with 128 bit AES (PAN is encrypted with FF1 mode of format preserving encryption). AES keys are created on the POI and a have configurable cryptoperiod. The AES keys are protected by 3072 bit RSA equivalent keys (decryption server public key, derived by IBE) for transmission to the Host System. AES card data keys are cached on the Host System. The cached AES keys may be written to an EFS volume, protected by a 128 bit AES key. The EFS key is provided by the Voltage SecureData Key Server. The Key Server protects or derives all keys for a District with a master secret for each key type. Master secrets are protected by the HSM master key (256 bit AES).
6A-1.2 *Cryptographic-key changes must be implemented for keys that have reached the end of their crypto-period (e.g., after a defined period of time and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (e.g., NIST Special Publication 800-57).*	Meets Requirement	Voltage SecureData provides key roll-over configurations for various keys: ▪ IBE keys use a validity period before new keys are derived ▪ Transaction key created on terminals can be configured for change interval Solution providers are responsible for configuring all host system and application account parameters.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6A-1.3 *Documentation describing the architecture (including all participating devices and cryptographic protocols), set-up and operation of the key-management solution must exist and must be demonstrably in use for all key-management processes.*	Meets Requirement	Voltage SecureData provides instructions for setting up devices, software, and key management services: ▪ *Voltage SecureData Appliance Installation Guide* ▪ *Voltage SecureData Payments Host SDK Developer Guide* ▪ *Voltage SecureData Payments Terminal SDK Developer Guide* ▪ *Voltage SecureData Architecture Guide* ▪ *Voltage SecureData Administrator Guide* ▪ *Voltage SecureData Atalla HSM Supplement* ▪ *Voltage SecureData Thales HSM Supplement* Solution providers are responsible for implementing, configuring, maintaining, and operating Voltage SecureData Payments in compliance with PCI P2PE v2.0 requirements.
6B-1.1 *Keys must be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys. Cryptographic keys or key components must be generated by one of the following:* • *An approved key-generation function of a PCI–approved HSM or POI device;* • *An approved key-generation function of a FIPS 140-2 Level 3 (or higher) HSM; or* • *An approved random number generator that has been certified by an independent laboratory to comply with NIST SP800-22*	Meets Requirement	Voltage SecureData Payments uses the HSM for generating or deriving all encryption keys, except for the symmetric transaction encryption key, which is generated by the POI device.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6B-2.1 through 6B-2.6 *Implement security controls, including dual control and tamper protection to prevent the unauthorized disclosure of keys/key components.*	Meets Requirement	Voltage SecureData Payments uses the HSM for generating or deriving Master Secrets, IBE Private Keys, and other keys used to protect transaction data. Traditional mechanisms, like clear-text components, are not used in Voltage SecureData Payments implementations. Transaction symmetric encryption keys are generated by POI devices, protected by the IBE public key for sharing with the Decryption Host. If cached to disk on the Decryption Host, they are stored encrypted. There are no manual processes where a person has any part or component of a key, although it is possible to access encrypted keys. HSM Master Keys are generated on HSM commissioning and are typically backed up to smartcards, per vendor instructions.
6B-3.1 *Written key-generation procedures must exist, and all affected parties (key custodians, supervisory staff, technical management, etc.) must be aware of these procedures. Procedures for creating all keys must be documented.*	Meets Requirement	Aside from the HSM Master Key, all keys are generated internally by Voltage SecureData without manual intervention. Voltage SecureData Payments logs record all key management activities. Voltage SecureData Payments does not require exchanging keys with other organization (typically KIFs or remote key services). Manually generated KEK and BDK are not used in SecureData Payments implementations.
6B-3.2 *Logs must exist for the generation of higher-level keys, such as KEKs exchanged with other organizations, and MFKs and BDKs.*	Meets Requirement	Aside from the HSM Master Key, all keys are generated automatically. Voltage SecureData Payments logs record all key management activities. Voltage SecureData Payments does not require exchanging keys with other organization (typically KIFs or remote key services). KEK and BDK are not used in Voltage SecureData Payments implementations.
6C-1.1 *Keys must be transferred either encrypted or within an SCD. If clear-text outside of an SCD as two or more components using different communication channels.*	Meets Requirement	HSM Master Keys must be generated and stored according to vendor guidelines. Voltage SecureData Payments eliminates the use of clear-text key components for managing keys. Requirements that govern clear-text key components are not applicable to Voltage SecureData Payments implementations.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6C-1.2 *A person with access to one component or share of a secret or private key, or to the media conveying this value, must not have access to other components or shares of this key or to any other medium containing other components or shares of this key that are sufficient to form the necessary threshold to derive the key.*	Supports Requirement	HSM Master Keys must be generated and stored according to vendor guidelines. Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person.
6C-1.4 *Public keys must be conveyed in a manner that protects their integrity and authenticity.*	Meets Requirement	Public keys are not conveyed. Voltage SecureData Payments uses IBE to derive public keys at terminals from parameters provided by the decryption environment. Solutions should demonstrate that POI verifies the integrity of parameter files that provide information for deriving Decryption Host public keys.
6C-2.1 *Any single clear-text secret or private key component/share must at all times be either:* • *Under the continuous supervision of a person with authorized access to this component, or* • *Locked in a security container (including pre-numbered, tamper-evident, authenticable packaging) in such a way that it can be obtained only by a person with authorized access to it, unauthorized access to it would be detected, or* • *Contained within a physically secure SCD.*	Minimizes Requirement	HSM Master Keys must be generated and stored according to vendor guidelines. Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person.
6C-2.2 through 6C-2.5 *Packaging or mailers (i.e., pre-numbered, tamper-evident packaging) containing clear-text key components are examined for evidence of tampering before being opened. Any sign of package tampering must result in the destruction and replacement of:* • *The set of components* • *Any keys encrypted under this (combined) key*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available for packaging or mailing.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6C-3.1 *All key-encryption keys used to encrypt for transmittal or conveyance of other cryptographic keys must be (at least) as strong as the key being sent, as delineated in Annex C, except as noted below for RSA keys used for key transport.* • *DEA keys used for encrypting keys must be at least double-length keys (have bit strength of 80 bits) and use the TDEA in an encrypt, decrypt, encrypt mode of operation for key-encipherment.* • *A double- or triple-length DEA key must not be encrypted with a DEA key of lesser strength.* • *TDEA keys shall not be used to protect AES keys.* • *TDEA keys shall not be used to encrypt keys greater in strength than 112 bits.* • *RSA keys encrypting keys greater in strength than 80 bits shall have bit strength of at least 112 bits.*	Meets Requirement	Voltage SecureData Payments encrypts transaction data with 128 bit AES (PAN use FF1 mode of format preserving encryption). AES keys are created on the POI and have a configurable cryptoperiod. The AES keys are protected by 3072 bit RSA equivalent keys (decryption server public key, derived by IBE) for transmission to the Host System. AES card data keys are cached on the Host System. The cached AES keys may be written to an EFS volume, protected by a 128 bit AES key. The EFS key is provided by the Voltage SecureData Key Server. Key Server protects or derives all key for a district with a master secret for each key type. Master secrets are protected by the HSM master key (256 bit AES).
6D-1 *Secret and private keys must be input into hardware (host) security modules (HSMs) and Point of Interaction (POI) devices in a secure manner.* *a) Unencrypted secret or private keys must be entered into cryptographic devices using the principles of dual control and split knowledge.* *b) Key-establishment techniques using public-key cryptography must be implemented securely.*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person. Manual key loading, except for recovering HSM Master Keys, is not applicable to Voltage SecureData Payments implementations.
6D-2 *The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person. Manual key loading, except for recovering HSM Master Keys, is not applicable to Voltage SecureData Payments implementations.
6D-3 *The mechanisms used to load secret and private keys—such as terminals, external PIN pads, key guns, or similar devices and methods—must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person. Manual key loading, except for recovering HSM Master Keys, is not applicable to Voltage SecureData Payments implementations.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6D-4 *The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person. Manual key loading, except for recovering HSM Master Keys, is not applicable to Voltage SecureData Payments implementations.
6D-5 *Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of components for managing all other keys. No key, or part of a key, managed by Voltage SecureData Payments is available unencrypted to a person. Manual key loading, except for recovering HSM Master Keys, is not applicable to Voltage SecureData Payments implementations.
6E-1 *Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems of two organizations or logically separate systems within the same organization.*	Minimizes Requirement	Voltage SecureData Payments eliminates the need for exchanging keys with other organizations and automates key protection for all uses within the same organization. Manual establishment or verification of keys for links between organizations or other systems is not applicable to Voltage SecureData Payments implementations.
6E-2 *Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another key or the operation of any cryptographic device without legitimate keys.*	Minimizes Requirement	Voltage SecureData Payments eliminates the need for exchanging keys with other organizations and automates key protection for all uses within the same organization. Voltage SecureData Payments provides automated key establishment and rotation and logs any synchronization errors.
6E-3 *Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.*	Meets Requirement	Voltage SecureData Payments provides for distinct service Identities that can be used to ensure that keys are never shared between test and production or any other service definitions useful for the solution provider.
6E-3.1 *Encryption keys must only be used for the purpose they were intended (i.e., key-encryption keys must not be used as PIN-encryption keys, PIN-encryption keys must not be used for account-data, etc.). This is necessary to limit the magnitude of exposure should any key(s) be compromised. Using keys only as they are intended also significantly strengthens the security of the underlying system.*	Meets Requirement	Voltage SecureData Payments has a built-in key hierarchy that ensures each key is used only for a single purpose and unique keys are used per device. Even the public keys that are derived for a specific decryption implementation have validity period, ensuring that they cannot be misused indefinitely. The *Voltage SecureData Architecture Guide* provides details on key use.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6E-3.2 *Private keys must only be used as follows:* - *For a single purpose—a private key must only be used for either decryption or for creating digital signatures, but not both (except for transaction-originating POI devices).* - *Private keys must never be used to encrypt other keys.*	Meets Requirement	Voltage SecureData Payments uses private keys only for decryption of Encryption Transmission Block (ETB) from terminals.
6E-3.3 *Public keys must only be used for a single purpose—a public key must only be used for either encryption or for verifying digital signatures, but not both (except for transaction-originating POI devices).*	Meets Requirement	Voltage SecureData Payments uses public keys only for encryption of ETB by terminals.
6E-4.1 *POI devices must each implement unique secret and private keys for any function directly or indirectly related to account-data protection. These keys must be known only in that device and in hardware security modules (HSMs) at the minimum number of facilities consistent with effective system operations.* *Disclosure of the key in one such device must not provide any information that could be feasibly used to determine the key in any other such device.*	Meets Requirement	Voltage SecureData Payments uses a random symmetric key generated by each terminal for transaction encryption. These are unique except by chance.
6E-4.3 *Keys that are generated by a derivation process and derived from the same Base (master) Derivation Key must use unique data for the derivation process as defined in ISO 11568 so that all such cryptographic devices receive unique initial secret keys. Base derivation keys must not ever be loaded onto POI devices—i.e., only the derived key is loaded to the POI device.*	Minimizes Requirement	Voltage SecureData Payments does not use DUKPT or similar scheme. BDK are not used and controls for DBK are not applicable.
6E-4.3 *Entities processing or injecting DUKPT or other key-derivation methodologies on behalf of multiple acquiring organizations must incorporate a segmentation strategy in their environments…*	Minimizes Requirement	Voltage SecureData Payments does not use Derived Unique Key Per Transaction (DUKPT) or similar scheme. BDKs are not used and controls for BDKs are not applicable.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6F-1.1 *Secret or private keys must only exist in one or more of the following forms:* • *At least two separate key shares or full-length components* • *Encrypted with a key of equal or greater strength as delineated in Annex C* • *Contained within a secure cryptographic device* *Note for hybrid decryption solutions: Clear-text Data Decryption Keys (DDKs) may temporarily be retained by the Host System in volatile memory for the purpose of decrypting account data.*	Meets Requirement	Voltage SecureData Payments generally protects keys with the HSM Master Key. However, the Decryption Server receives symmetric transaction encryption keys from each POI device in the ETB and retains those keys in a memory cache. There is also an optional disk cache, which stores the keys in an encrypted file in the event a restart of the Decryption Host is needed.
6F-1.2 *Wherever key components are used, they have the following properties…*	Minimizes Requirement	Voltage SecureData Payments eliminates the use of clear-text key components for managing keys. Requirements that govern clear text key components are not applicable to Voltage SecureData Payments implementations.
6H-1.1 *The Data Decryption Keys (DDKs) used in software to decrypt account data must have defined usage limits. This can be achieved through the use of either one of the following approaches:* • *Each DDK must have a defined usage period (cryptoperiod) based on a formal risk assessment and industry guidance as provided in NIST SP800-57, ISO TR 14742 and NIST SP800-131. The cryptoperiod defines the duration of time that the DDK may be used to decrypt account data, defined either as a maximum threshold of transactions, or hours, or both (e.g., 1024 transactions or 24 hours, whichever is reached first).* • *Upon reaching the defined usage threshold, the DDK must not be used for further transaction processing and must be securely erased from memory of the Host System.* *OR* • *DDKs are unique per transaction. Each DDK is erased from the host memory upon completion of the decryption process.*	Meets Requirement	The terminal application using the Voltage SecureData Payments Terminal SDK can create a new random transaction key on any interval or threshold. On receiving a new random key in an ETB, the Host System discards the previous random key for that terminal. Voltage SecureData Payments Host SDK also provides mechanisms for purging random transaction keys that have not been recently used.
6H-1.2 *DDKs must be erased from the Host System volatile memory via a mechanism that ensures the key cannot be recovered or reconstructed.*	Meets Requirement	Voltage SecureData Payments Host SDK replaces keys or zeroized memory locations that are not immediately reused.

PCI P2PE REQUIREMENT	IMPACT	APPLICABILITY
6H-1.3 *If the DDK is generated from a master key, the following conditions apply:* - *A one-way derivation process must be used.* - *The DDK must never be generated as a variant of the HSM master file key.* *The master key used to generate the DDK must be dedicated to generating DDKs.*	Minimizes Requirement	DDK are generated by the POI RNG and not derived from a master key.
6H-1.4 *The DDK must be encrypted between the HSM and the Host System, e.g., using a fixed transport key or a cryptographic protocol. The method of encryption used must maintain the security policy to which the HSM was approved (either FIPS140-2, Level 3 or higher, or approved to the PCI HSM standard).*	Meets Requirement	DDK are only communicated between the POI and the Host System. They are protected by the 3072-bit IBE public key of the decryption service.
6H-1.5 *The encryption mechanism used to protect the DDK between the HSM and the Host System:* - *The encryption key must be equal or greater in strength than the key it protects.* - *The encryption key must be unique for each Host System.* - *The encryption key must only be used to encrypt the DDK during transmission between the HSM and the Host System, and not used to encrypt/transmit any other cryptographic key, or for any other purpose.* - *The encryption key must have a defined cryptoperiod based on the volume of keys it transports and industry recommendations/best practices.*	Meets Requirement	DDK are only communicated between the POI and the Host System. They are protected by the 3072-bit IBE public key of the decryption service. The terminal application using the Voltage SecureData Payments Terminal SDK can create a new random transaction key on any interval or threshold.

NESA FOR SOLUTIONS USING VOLTAGE SECUREDATA PAYMENTS

The *Assessment Guidance for Non-Listed Encryption Solutions*, released by PCI in November 2016, is guidance intended to help acquirers evaluate the relative security of encryption solutions that reduce the risk of breach of card-present payments, but have not be validated for PCI P2PE. Acquirers may choose to permit reduced reporting for merchants using a secure, if not PCI P2PE validated encryption solution.

Because the NESA Guideline lists minimum requirements for solutions, including POI requirements and the requirement that the decryption environment meet PCI P2PE Domain 5 and relevant Domain 6 controls, there has been confusion that NESA has established a new category of "NESA Compliant" solutions. PCI has clearly communicated to the QSA community that this is not the case. As the name implies, NESA is both an assessment and a guideline. The decision on applicable DSS controls for merchants using these solutions is completely up to their acquirer.

Acquirers have been relying on the assessment and recommendation of the merchant's QSA. The only PCI-compliant means of reducing merchant scope for card-present payments are PCI P2PE solutions. PCI became concerned that all QSAs are not qualified to evaluate encryption solutions because it requires knowledge not required for QSAs. Acquirers have been left with third party whitepapers with inconsistent testing criteria, vendor technical papers, and field testing to make these risk decisions. This lack of an assessment standard had lead many acquirers to deny reduced reporting for all encryption solutions, or at least all solutions except their own. A NESA must be conducted by a P2PE QSA, against a consistent standard, and presented is a consistent format. This provides acquirers with a fair evaluation of a solution's security to support their risk decision on merchant DSS reporting.

While acquirers are not held the requirements in the NESA guidance, the requirements clearly communicate what the PCI P2PE Working Group considers the minimum standards for a card-present encryption solution to be considered secure. The requirements in the NESA Guidance have a major impact on encryption solutions using Voltage SecureData Payments:

1. The merchant is using PCI-listed PTS POI v2 (or higher) devices for the acceptance and encryption of payment brand account data. (Note: PTS POI v2 are no longer permitted for new deployments, as of April 2017.)
2. The merchant never has access to account data encryption/decryption keys.
3. The merchant never has access to clear-text account data transmitted outside of the device.
4. The solution is expected to meet all the applicable requirement in Domains 5 and 6 in the current PCI P2PE standard.
5. Merchant-managed solutions are excluded.

Permitting all PTS POI v2 (or higher) enables a solution to support a broad range of POI, rather that only POI that support the Voltage SecureData Payments Terminal SDK in SRED.

With non-merchant operated Voltage SecureData Payments solutions, merchants cannot access either encryption/decryption keys or clear-text account data.

The previous section, *Meeting PCI P2PE requirements using Voltage SecureData Payments*, describes applicable P2PE Domain 5 and 6 controls and how they may be met with a Voltage SecureData Payments solution.

Merchants who implement their own encryption solutions will continue to need annual acquirer approval for any DSS reporting impact. The NESA reporting template may be used to present an assessment of their solution to their acquirer as long as it is clear that the solution is outside of the scope in the PCI *Assessment Guidance for Non-Listed Encryption Solutions* document.

COMPLETING THE NON-LISTED ENCRYPTION SOLUTION ASSESSMENT (NESA) SUMMARY

The *Non-Listed Encryption Solution Assessment (NESA) Summary Documentation Template*, available on the PCI website, is used for reporting NESA results.

Information used to describe the solution:

- P2PE Assessor Company Name
- Company Name for the non-listed encryption solution provider
- Description of the non-listed encryption solution provider (e.g., payment gateway, acquirer, multi-acquirer payment processor, etc.)
- Non-listed encryption solution Name and Version Number, as applicable
- Brief Description of product
- Document Name and versioning for the instruction manual
- Additional comments, if needed

Scoping Criteria:

- List of PCI-approved POI(s) assessed, including:
  - PTS Approval Number
  - Make/Model
  - Hardware #
  - Firmware #
- All Applications on POI (Application Name and Version)
- Description of the non-listed encryption solution implementation(s) tested, including hardware and software dependencies:
- Additional comments, if needed

If the NESA will be attested to by a P2PE QSA, it must meet the following:

- The “Scoping Criteria” defined in the Assessment Guidance for Non-listed Encryption Solutions has been met;
- Compliance to P2PE Domains 5 and 6 have been fully validated; and
- Compliance to P2PE Domains 1, 2, and 3 have been validated as documented in section 1.4, P-ROV Findings by Domain, below.

For P-ROV Findings by Domain, Voltage SecureData Payments has 1 or more impacts:

- Full Compliance: Voltage SecureData Payments technology or process conforms to the requirement. The encryption solution may use Voltage SecureData Payments to meet the requirement. The Provider needs to implement Voltage SecureData Payments per the instructions under "Applicability" to be compliant.
- Non-Compliant: Voltage SecureData Payments features support a secure encryption solution, but do not meet the P2PE requirement, which is optional for a NESA.
- No Impact: Voltage SecureData Payments does not impact requirement. The compliance status of the requirement is solely the responsibility of the encryption solution provider.

PCI P2PE Requirement	Findings	Applicability
Domain 1: Encryption Device and Application Management		
1A Account data must be encrypted in equipment that is resistant to physical and logical compromise.		
1A-1 PCI-approved POI devices with SRED are used for transaction acceptance.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Voltage SecureData Payments relies on AES FPE FF1 format preserving encryption and key generation implemented as part of a terminal's SRED functionality. Solution providers need to verify from vendors that these functions are part of the SRED-tested firmware for any POI supported by a solution. Terminals are available that have included Voltage SecureData Payments Terminal SDK in their SRED firmware. Any terminal that is PCI PTS v2 or higher that supports the Voltage SecureData Payments Terminal SDK may be used in a non-compliant solution.
1A-2 Applications on POI devices with access to clear-text account data are assessed per Domain 2 before being deployed into a P2PE solution.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Applications on the POI that are include with the Voltage SecureData Payments Terminal SDK have clear-text account data. For Full Compliance, these applications must have a completed Domain 2 assessment. Non-Compliant solutions are permissible for encryption solutions, but are regarded as a higher risk. POI that have the Voltage SecureData Payments Terminal SDK implemented in SRED firmware may eliminate the need for an application with access to clear-text account data.
1B Logically secure POI devices.		
1B-1 Solution provider ensures that logical access to POI devices deployed at merchant encryption environment(s) is restricted to authorized personnel.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility

PCI P2PE Requirement		Findings	Applicability
1B-2	*Solution provider secures any remote access to POI devices deployed at merchant encryption environments.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility
1B-3	*The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility
1B-4	*Solution provider implements procedures to secure account data when troubleshooting*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility
1B-5	*The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility
1C	**Use P2PE applications that protect PAN and SAD.**		
1C-1	*Applications are implemented securely, including when using shared resources and when updating applications and application functionality.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility. Voltage SecureData Payments Terminal SDK does not provide any whitelisting or BIN exclusion functionality.
1C-2	*All applications/software without a business need do not have access to account data.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
1D	**Implement secure application-management processes.**		
1D-1	*Integrity of applications is maintained during installation and updates.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
1D-2	*Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
1E	**Component providers *ONLY*: report status to solution providers**		
1E-1	*For component providers of encryption-management services, maintain and monitor critical P2PE controls and provide*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.

PCI P2PE Requirement	Findings	Applicability
reporting to the responsible solution provider.		
Domain 2: Application Security		
2A Protect PAN and SAD		
2A-1 The application executes on a PCI-approved POI device with SRED enabled and active.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Voltage SecureData Payments relies on AES FPE FF1 format preserving encryption and key generation implemented as part of a terminal's SRED functionality. Solution providers need to verify from vendors that these functions are part of the SRED-tested firmware for any POI supported by a solution. Terminals are available that have included Voltage SecureData Payments Terminal SDK in their SRED firmware. Any terminal that is PCI PTS v2 or higher that supports the Voltage SecureData Payments Terminal SDK may be used in a non-compliant solution.
2A-2 The application does not store PAN and/or SAD for any longer than business processes require.	☒ Full Compliance ☐ Non-Compliant ☐ No Impact	Voltage SecureData Payments Terminal SDK does not store PAN or SAD data. It is held in volatile memory until encrypted data is produced, then securely deleted.
2A-3 The application does not transmit clear-text PAN and/or SAD outside of the POI device, and only uses communication methods included in the scope of the PCI-approved POI device evaluation.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Voltage SecureData Payments Terminal SDK does not implement any whitelisting functionality.
2B Develop and maintain secure applications.		
2B-1 The application is developed and tested according to industry-standard software development life cycle practices that incorporate information security.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Voltage SecureData Payments Terminal SDK development processes meet all PCI P2PE Domain 2 requirements. Voltage SecureData Payments Terminal SDK undergoes risk-assessment as a regular part of its development process.
2B-2 The application is implemented securely, including the secure use of any resources shared between different applications.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Voltage SecureData Payments Terminal SDK uses only documents interfaces for exchanging data with applications.
2B-3 The application vendor uses secure protocols, provides guidance on their use, and performs integration testing on the final application.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Voltage SecureData key use is described in *Voltage SecureData Architecture Guide*. Terminals are provided with a signed parameter block used to derive the solution provider's public key (3072 bit RSA), using IBE. The integrity of this public key is assured by the integrity controls on the parameter block and derivation process. The SRED key generation function of the terminal is used to generate a 128 bit AES symmetric key for encrypting transaction data. This key is stored in the terminal's SRED

PCI P2PE Requirement	Findings	Applicability
		key storage. The symmetric key is protected by the public key for transmission to the solution provider. If Voltage SecureData may be configured to use other key lengths which may not be compliant.
2B-4 Applications do not implement any encryption functions in lieu of SRED encryption. All such functions are performed by the approved SRED firmware of the POI device.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Applications need to ensure that encryption SRED functions are used for account data. This can be implemented either by using a POI that has Voltage SecureData Payments Terminal SDK implemented as part of its SRED functionality or by defining AES and RNG alternate implementations (per *Voltage SecureData Payments Terminal SDK Developer Guide,* Annex A) to use terminal SRED functions.
2C Implement secure application-management processes.		
2C-1 New vulnerabilities are discovered and applications are tested for those vulnerabilities on an ongoing basis.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Voltage SecureData Payments Terminal SDK development processes meet all PCI P2PE Domain 2 requirements. It is tested for vulnerabilities with both manual and automated processes. Application developers are notified of all Voltage SecureData Payments Terminal SDK updates and discovered vulnerabilities.
2C-2 Applications are installed and updates are implemented only via trusted and cryptographically authenticated processes using an approved security mechanism evaluated for the PCI-approved POI device.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
2C-3 Maintain instructional documentation and training programs for the application's installation, maintenance/upgrades, and use.	☒ Full Compliance ☒ Non-Compliant ☐ No Impact	Complete implementer documentation for Voltage SecureData Payments Terminal SDK is provided and revised with each release.
Domain 3: P2PE Solution Management		
3A P2PE solution management		
3A-1 The solution provider maintains documentation detailing the P2PE solution architecture and data flows.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3A-2 The solution provider manages and monitors status reporting from P2PE component providers.	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.

PCI P2PE Requirement		Findings	Applicability
3A-3	*Solution provider implements processes to respond to notifications from merchants, component providers and/or third parties, and provide notifications about any suspicious activity involving the P2PE solution.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3A-4	*If the solution provider allows a merchant to stop P2PE encryption of account data, the solution provider manages the related process for merchants*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3B	**Third-party management**		
3B-1	*The solution provider facilitates and maintains formal agreements with all third parties contracted to perform P2PE functions on behalf of the solution provider.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3B-2	*Solution provider secures any remote access to POI devices deployed at merchant encryption environments.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3B-3	*The solution provider implements procedures to protect POI devices and applications from known vulnerabilities and securely update devices.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3B-4	*Solution provider implements procedures to secure account data when troubleshooting*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3B-5	*The P2PE solution provides auditable logs of any changes to critical functions of the POI device(s).*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.
3C	**Creation and maintenance of *P2PE Instruction Manual* for merchants**		
3C-1	*Solution provider develops, maintains, and disseminates a P2PE Instruction Manual to merchants.*	☐ Full Compliance ☐ Non-Compliant ☒ No Impact	Encryption solution provider responsibility.

P2PE ASSESSOR'S RECOMMENDATION(S) FOR POSSIBLE PCI DSS CONTROL REDUCTIONS

The *Assessment Guidance for Non-Listed Encryption Solutions* describes the P2PE assessor's responsibilities as:

- The merchant/merchant's QSA must validate that the non-validated encryption solution was implemented in accordance with the instruction manual provided by the solution provider and in a PCI DSS compliant manner;
- The merchant/merchant's QSA must validate that there are no additional payment acceptance channels or the presence of any clear-text cardholder data within the merchant environment;

A NESA report for an encryption solution will include a table of DSS controls that are recommended for control reduction for merchants using the solution. For solutions using Voltage SecureData Payments a complete description of merchant impacts and applicable DSS controls is available in the *Voltage SecureData Payments PCI DSS v3.2 Control Applicability Assessment White Paper.*

CONCLUSIONS

Voltage SecureData Payments is an effective technology platform for implementing PCI P2PE solutions. It offers distinct advantages over traditional DUKPT systems, including:

1. Voltage IBE allows terminals to be enrolled during installation, without needing a key injection facility.
2. The key management features of the Voltage SecureData Appliance simplify and eliminate most common datacenter key management processes.

Careful planning and implementation is needed to ensure the solution will meet the additional requirements for a hybrid decryption environment.

Terminals and terminal applications need to be carefully selected to ensure that SRED functions are used for transaction encryption, key creation, and key storage.

ABOUT THE AUTHOR

Tim Winston, PA-QSA(P2PE), CTGA, CISSP, CISA | Payment Processors & P2PE Principal

With decades of information technology architecture and security experience, Tim is responsible for technical leadership of Coalfire's P2PE and payment encryption advisory and assessment practice.

Published September 2017.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.