WHITE PAPER

HPE SECUREDATA PAYMENTS PCI DSS V3.2 CONTROL APPLICABILITY ASSESSMENT

TIM WINSTON | PCI/P2PE PRACTICE DIRECTOR

PREPARED FOR:

Hewlett Packard Enterprise

COALFIRE

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Hewlett Packard Enterprise (HPE) engaged Coalfire Systems, Inc. (Coalfire) as a respected Payment Card Industry (PCI) Qualified Security Assessor (QSA) to conduct an independent technical assessment of their HPE SecureData Payments solution. Coalfire did not conduct technical testing for this assessment. The assessment was to identify the potential impact to the number of PCI DSS 3.2 controls applicable to merchants using encryption solutions based on HPE SecureData Payments.

In this paper, Coalfire will describe the HPE SecureData Payments solution and the particular requirements it impacts within PCI DSS scope.

ABOUT HPE SECUREDATA PAYMENTS

The HPE SecureData Payments solution is intended to increase the security of card-present payments without impacting the buyer experience. Solutions based on HPE SecureData Payments reduce merchant risk of losing credit card data and potentially reduce the number of PCI DSS controls applicable to the retail payment environment substantially.

HPE 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 the solution provider, typically a payment service. Even a compromise of the point-of-sale (POS) system does not expose customers' sensitive data.

Merchants can also realize reduction in DSS compliance scope by implementing their own HPE SecureData Payments solution.

AUDIENCE

This assessment white paper has three target audiences:

1. First, merchants using HPE SecureData Payments to create proprietary encryption solutions for card-present payments
2. The second is service providers, like processors, and payment services that are developing card-present encryption services that utilize HPE SecureData Payments
3. The third is the QSA and internal audit community that is evaluating solutions in both merchant and service provider environments using the HPE SecureData Payments solution

ASSESSMENT SCOPE

HPE contracted with Coalfire to provide an independent compliance impact review of the HPE SecureData Payments solution. The intent of this assessment was to analyze the impact on PCI DSS scope of applicable controls for merchants that implement an HPE SecureData Payments solution for their card-present sales.

ABOUT HPE SECUREDATA PAYMENTS

HPE SecureData Payments has three components:

1. **HPE SecureData Appliances,** which manages private keys for data decryption and connects to hardware security modules (HSM) for the highest security private key storage and key management
2. **HPE SecureData Payment Terminal software development kit (SDK),** a library that may be compiled into an encryption solution's POI terminal application or POI firmware
3. **HPE SecureData Payment Host SDK,** a library that provides decryption and key management services with the HPE SecureData Appliance

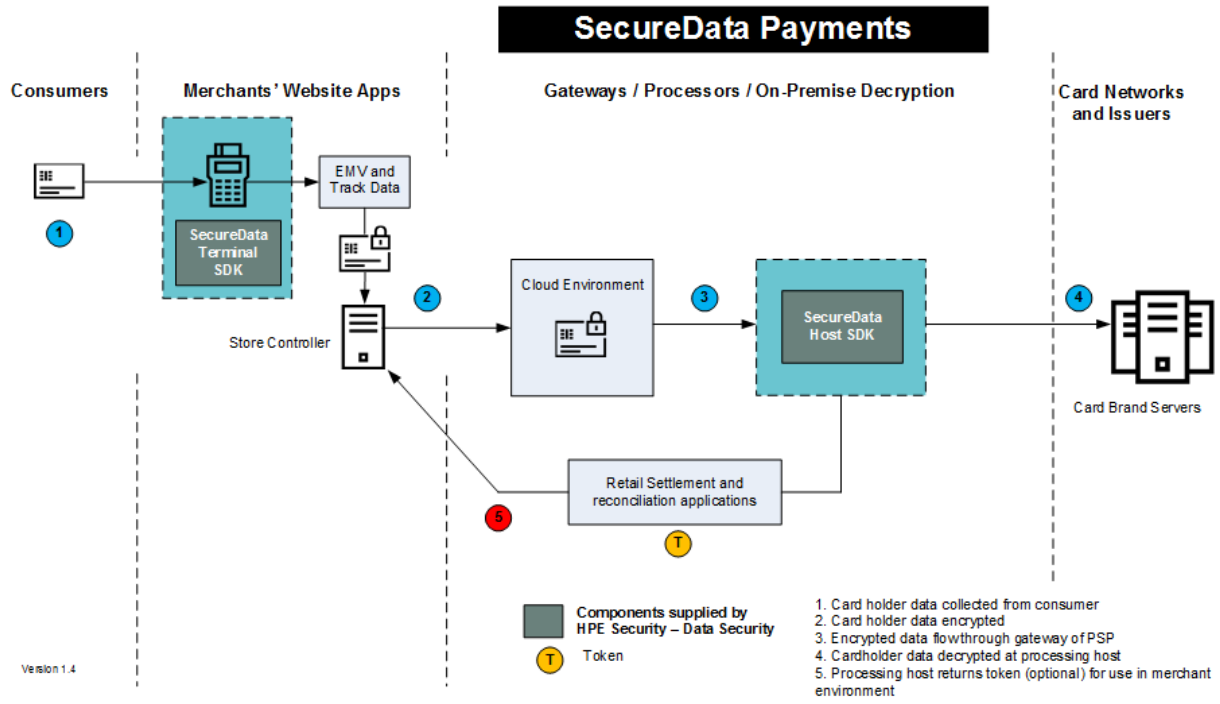

Figure 1: Generalized payment flow with cardholder data encryption and tokenization

The HPE SecureData Payments Terminal SDK is delivered in source code, and the HPE SecureData Payments Host SDK is delivered in libraries/packages to support a range of devices and servers. Solution providers can develop additional features to create complete card-present encryption solutions.

HPE SecureData Payments is distinguished from other encryption mechanisms by two breakthrough technologies:

1. With HPE 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—such as the Luhn checksum and field separators—are maintained, and 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 is a mode of advanced encryption standard (AES) encryption, as described by the NIST SP800-38G Standard and accepted by the PCI Security Standards Council (SSC) as strong encryption.

2. HPE Identity-Based Encryption (IBE) is a breakthrough in key management that 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. HPE IBE also enables end-to-end encryption from swipe-to-processor and swipe-to-trusted-merchant applications. IBE is an ISO (ISO/IEC 18033-5) and Institute of Electrical and Electronics Engineers (IEEE 1363.3) standard for asymmetric encryption key management.

HPE SecureData Payments is a secure, versatile, and scalable encryption solution for card-present payments.

PCI DSS IMPACT

OVERVIEW

The benefit of using an HPE SecureData Payments solution is that the risk of loss of sensitive credit card data is all but eliminated. Sensitive credit card data is removed from the POS systems and network and cannot be exposed, even in serious breaches. Because implementations rely on encryption on POI devices that are designed and tested for security, and decryption takes place in a highly controlled environment, the effort to demonstrate PCI DSS compliance for retail networks is greatly reduced.

MERCHANT PCI COMPLIANCE SCOPE AND ENCRYPTED TRANSACTIONS

The PCI DSS guidelines require compliance within a merchant's cardholder data environment (CDE), which includes all systems, connecting systems, and devices that store, transmit, or process cardholder data. Sensitive cardholder data (CHD) that has been encrypted with secure methods and an encryption key that is never in the merchant's possession is still in scope of DSS, but many DSS controls can be considered "not applicable." PCI DSS controls that remain applicable for a specific implementation are determined by the impact of the control on the security of sensitive credit card information. For example, Requirement 9.9, which requires periodic inspections of POI devices for skimmers or other tampering, is clearly still needed to prevent data from being stolen by skimmers.

The relevant high-level findings from Coalfire's technical review of HPE SecureData Payments are as follows:

- A properly designed and deployed HPE SecureData Payments solution has an impact on the assessment of **15 of PCI's 242 requirements, or 94%,** for the retail environment for merchants using the service provider's solution.
- An HPE SecureData Payments solution reduces the risk of consumer CHD compromise and removes exposure of plain text CHD in the retail environment by encrypting CHD immediately on entry.
- Merchants maintaining their own trusted host environment are still subject to all PCI DSS controls. However, most controls will apply on to the HPE SecureData SDK (decryption server) host (decryption server), HPE SecureData KeyServer, HSMs, network devices providing network access control to that environment, and systems that process transactions after decryption. The majority of controls (**up to 94%**) will not apply to retail networks and systems if appropriate separation of duties is implemented to protect encryption keys. This means that full DSS compliance may be reduced from all of the systems in the card-present environment to a handful of centrally located systems.
- QSAs and acquiring banks may make a risk-based determination to completely remove the merchant retail environment from the scope of PCI DSS, thereby further reducing the cost of validating PCI DSS compliance, when merchants use a trusted host environment solution provider.

Which DSS controls remain applicable is also determined differently depending on whether or not the specific implementation of the HPE SecureData Payments solution is part of a PCI point-to-point encryption (P2PE) listed solution.

For PCI-listed P2PE solutions, that answer is straightforward: Applicable controls are listed in PCI SAQ-P2PE. These controls mainly concern requiring merchants to monitor the compliance of their solution provider and follow the P2PE Implementation Guide (PIM) provided by their solution provider.

HPE SecureData Payments may be implemented by organizations and taken through a PCI P2PE v2 validation. However, for merchants or processors that do not wish to undertake this process, encryption solutions that are not PCI P2PE listed may still allow significant reduction in applicable controls, if the merchant's acquirer agrees to the reduction. While this is completely at the discretion of the acquirer, the applicable controls will at least include the controls listed in SAQ-P2PE plus additional controls that are needed to secure sensitive credit card data or demonstrate the proper implementation of the solution.

Critical factors in determining the scope of PCI DSS controls that are applicable to any network involved in processing, transmitting, or storing encrypted sensitive credit card data, including primary account number (PAN), card verification values (CVVs), and magnetic track data, are:

1. Encryption strength
2. Separation of encryption keys from encrypted data

HPE SecureData Payments uses encryption algorithms and encryption key management that are proven to be secure and meeting PCI security key requirements. They use key strength of 128-bit advanced encryption standard (AES) format-preserving encryption (FPE) and Rivest-Shamir-Adleman (RSA) key size of 3072 bit identity based encryption (IBE). This satisfies the technical requirements for both factors. However, HPE SecureData Payments Host SDK runs on host systems and uses data decryption keys. This requires that those systems have demonstrably effective controls for access to decryption keys by both authorized and unauthorized personnel.

For service providers, these controls are tested during their PCI service provider report on compliance (ROC) assessment. Merchants can rely on a service provider's attestation of compliance (AOC) that those controls are effectively functioning. Since the merchant and service provider are separate legal entities, this also ensures key administrators, who work for the service provider, do not have access to encrypted traffic on merchant networks. This allows the service provider to take total responsibility for PCI DSS key management controls, significantly reducing controls that apply to the merchant's point-of-sale (POS) systems and networks.

Merchants developing and maintaining their own card-present encryption solution may still reduce the PCI DSS controls applicable to their POS systems and networks, but will need to demonstrate compliance with key management controls as well as controls pertaining to the system integrity of the decryption host.

Merchants deploying HPE SecureData Payments may also look at hybrid options to take advantage of the additional scope reduction in the service provider model. For example, if the key management system is managed by a third party entity (e.g., hosted or remotely managed), then the solution may be assessed under the service provider scope reduction assessment. The solution is flexible for such approaches and adaptable to a merchants' specific needs.

There will always be certain controls for PCI compliance that must be independently assessed in any merchant's environment, and PCI compliance will always apply to a merchant if CHD is transmitted, processed, or stored anywhere in their physical environment.

KEY MANAGEMENT ARCHITECTURE

PCI DSS 3.2 added a Requirement 3.5.1 for service providers:

Maintain a documented description of the cryptographic architecture that includes:

- Details of all algorithms, protocols, and keys used for the protection of CHD, including key strength and expiry date
- Description of the key usage for each key
- Inventory of any HSMs and other SCDs used for key management

This is a best practice until January 31, 2018, after which it becomes a requirement.

HPE SecureData Payments satisfies this requirement by providing a complete cryptographic architecture:

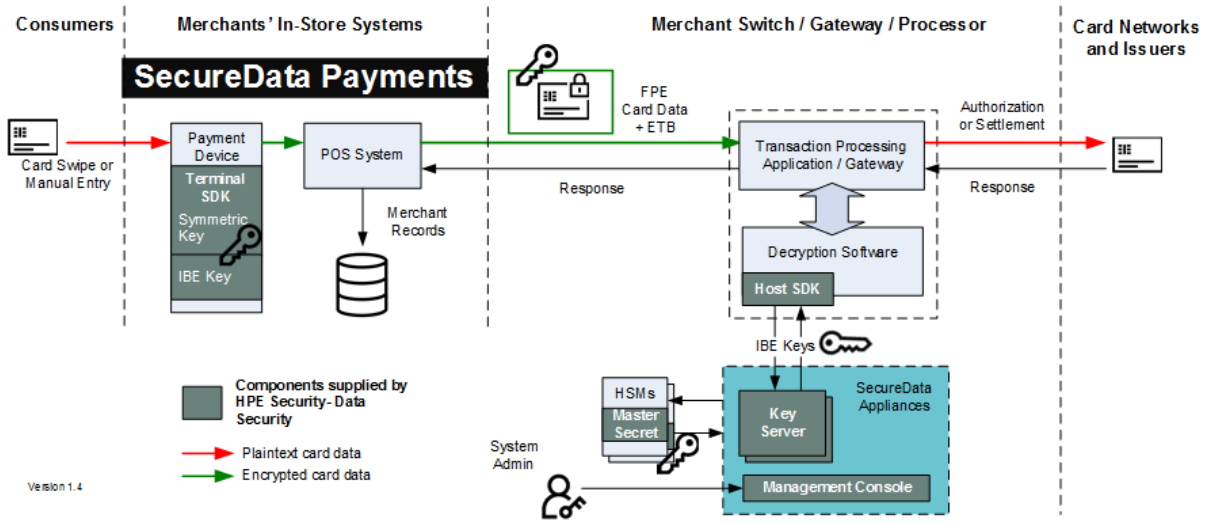

Figure 2: Key architecture

KEY NAME	USAGE	ALGORITHMS/ STRENGTH	KEY ROLLOVER	KEY SECURED BY
Symmetric (FPE) key	Encryption of account data	AES FFX mode / 128 bits	Automated within each terminal and uses randomly generated values at the start of each (configurable) cryptoperiod	IBE (ETB) key
IBE (ETB) key	Asymmetric key pair for key IBE exchange	BB1 / 3072 bit (RSA equivalent strength)	New IBE keys get generated dynamically whenever a new ETB gets generated, which happens whenever the data key is rolled (once per cryptoperiod)	Master secret key
Master secret key	HSM master key	AES / 256 bit	Use standard management console key group rollover (at customer's control)	Stored on HSM and secure backup smartcards

Note that service providers using HPE SecureData will need to configure cryptoperiods for each key that is appropriate to their implementation.

In addition to this information, service providers will need to supply an inventory of HSM(s) and HPE SecureData appliances for their DSS assessment.

SUMMARY CHART OF POTENTIAL IMPACT ON MERCHANT AUDIT APPLICABLE CONTROLS TABLE

As described in the previous section, PCI DSS controls that remain applicable for the DMZ web application depend on whether the merchant is using an HPE SecureData Web-based solution from a service provider or maintaining its own solution.

Legend:

- Merchant is using a service provider managed e-commerce encryption
- Merchant manages card-present encryption solution
- Merchant manages using a service provider for decryption

PCI DSS REQUIREMENT SECTION	MAJOR APPLICABLE CONTROL REDUCTION	MODERATE APPLICABLE CONTROL REDUCTION	LOW APPLICABLE CONTROL REDUCTION	NO IMPACT TO APPLICATION CONTROLS
1	● ●	●		
2	● ●	●		
3	● ●		●	
4	● ●	●		
5	● ●	●		
6	● ●	●		
7	● ●		●	
8	● ●	●		
9		● ● ●		
10	● ●	●		
11		● ●	●	
12			● ● ●	

KEY TO POTENTIAL IMPACT ON APPLICABLE CONTROLS TABLE

Applicable control level	Description
1	Control is not applicable for a properly and exclusively implemented solution based on HPE SecureData Payments. The QSA should determine if the control applies to other sources of CHD.
2	Properly implemented, this solution reduces, but does not eliminate, the applicability of this control. The QSA should determine to what extent the control applies.
3	Control is applicable. Normal testing procedure should be used.

POTENTIAL IMPACT ON APPLICABLE CONTROLS TABLE

Note: If a specific requirement is not listed, then that requirement is either not or only slightly impacted by proper implementation of the HPE SecureData Payments solution, and will probably still be applicable during a PCI DSS 3.2 audit.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
Build and maintain a secure network and systems			
Requirement 1: Install and maintain a firewall configuration to protect CHD			This requirement mostly lies outside of HPE SecureData Payments. Regardless, nothing within HPE SecureData Payments prevents a vendor from using a properly configured firewall. HPE SecureData Payments uses only standard communications protocols and ports.
1.1 Establish and implement firewall and router configuration standards.	**2**	**3**	1.1.2 and 1.1.3: Merchants should still diagram the network and the data flow of the locations where P2PE will be utilized to enable QSA to verify that the solution is properly implemented. For merchant-managed environments, a firewall is required to enforce network access control for the decryption host, HPE SecureData Appliance, and HSM.
1.2 Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the CDE.	**1**	**3**	For merchant-managed environments, a firewall is required to enforce network access control for the decryption host, HPE SecureData Appliance, and HSM. Even in that case, this control will not apply to POS networks, if appropriate separation of duties is implemented to protect encryption keys.
1.3 Prohibit direct public access between the Internet and any system component in the CDE.	**2**	**2**	1.3.3: Merchants should not permit direct unrestricted inbound Internet access to the POIs. For merchant-managed environments, a firewall is required to enforce network access control for the decryption host, HPE SecureData Appliance, and HSM.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.	**1**	**3**	For merchants that have any networks that transport unencrypted sensitive credit card data, this control must apply.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
1.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: • Documented • In use • Known to all affected parties	**3**	**3**	Requirements concerning policies are always applicable.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			HPE SecureData Payments dramatically reduces the scope of this requirement, because so much of the merchant's network can be put out of scope of PCI DSS.
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	**1**	**3**	For merchant-managed environments, device configuration standards requirements are applicable to enforce secure configuration for the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks, if appropriate separation of duties is implemented to protect encryption keys.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	**1**	**3**	For merchant-managed environments, device configuration standards requirements are applicable to enforce secure configuration for the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks, if appropriate separation of duties is implemented to protect encryption keys.
2.3 Encrypt all non-console administrative access using strong cryptography.	**1**	**3**	For merchant-managed environments, device configuration standards requirements are applicable to enforce secure configuration for the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	**1**	**3**	For merchant-managed environments, the requirement is applicable for the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
2.5: Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
2.6: Shared hosting providers must protect each entity's hosted environment and CHD. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	**N/A**	**3**	Shared hosting providers are always subject to this requirement.
Protect cardholder data			
Requirement 3: Protect stored CHD			
3.1 Keep CHD storage to a minimum by implementing data retention and disposal policies, procedures, and processes.	**3**	**3**	PCI DSS policy requirements are always applicable, even if cardholder data is not stored. In that case the policy would prohibit storage of sensitive credit card data. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all storage controls.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all storage controls.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all storage controls.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all storage controls.
3.5 Document and implement procedures to protect keys used to secure stored CHD against disclosure and misuse.	**2**	**3**	Because this requirement is about documentation, it lies outside the responsibility of HPE SecureData Payments for merchants using a service provider solution. However, this requirement is partially covered because the merchant does not have access to the encryption keys at all. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all key protection controls.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of CHD.	**2**	**3**	Because this requirement is about documentation, it lies outside the responsibility of HPE SecureData Payments for merchants using a service provider solution. However, this requirement is partially covered because the merchant does not have access to the encryption keys at all. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all key protection controls.
3.7 Ensure that security policies and operational procedures for protecting stored CHD are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable. It is expected that the policy for cardholder data is that sensitive CHD is not stored or transmitted for service provider solutions.
Requirement 4: Encrypt transmission of CHD across open, public networks			

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
4.1 Use strong cryptography and security protocols to safeguard sensitive CHD during transmission over open, public networks.	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the CDE and subject to all secure transmission controls. Even in that case, this control will not apply to POS networks, if appropriate separation of duties is implemented to protect encryption keys.
4.2 Never send unprotected PANs by end-user messaging technologies.	**1**	**3**	In a properly configured HPE SecureData Payments service provider deployment, the merchant has no access to unprotected PANs at all. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE and subject to all secure transmission controls.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable. It is expected that the policy for CHD is that sensitive CHD is not stored or transmitted under any conditions.
Maintain a vulnerability management program			
Requirement 5: Protect all systems against malware and regularly update antivirus software or programs			This requirement does not apply to HPE SecureData Payments, but there is nothing within HPE SecureData Payments that would prevent an antivirus program from running properly. A vendor can fulfill PCI DSS Requirement 5 while properly implementing an HPE SecureData Payments solution.
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems and subject to all antivirus controls. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
5.2 Ensure that all antivirus mechanisms are maintained.	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems and subject to all antivirus controls. Even in that case, this control will not apply to POS networks, if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
5.3: Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time period.	**1**	**3**	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems and subject to all antivirus controls. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
5.4: Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable. It is expected that the policy for CHD is that sensitive CHD is not stored or transmitted under any conditions.
Requirement 6: Develop and maintain secure systems and applications			This requirement is extremely important, because HPE SecureData Payments requires an application to be built using HPE SecureData Payments. HPE SecureData itself meets all of the standards mandated by this requirement. The encryption solution provider must assure merchants that Requirement 6 is met for all systems and applications in the solution.
6.1 Establish a process to identify security vulnerabilities using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	**1**	**3**	For service provider solutions, merchants must respond to all notifications from the encryption solution provider immediately and take directed actions. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems and subject to all secure system management controls. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	1	3	For service provider solutions, merchants must respond to all notifications from the encryption solution provider immediately and take directed actions. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems and subject to all secure system management controls. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely.	1	3	For merchant-managed solutions, CHD encrypted at POI is decrypted within the CDE on decryption host systems with custom applications that use the HPE SecureData Host SDK. These applications are subject to all secure software lifecycle controls. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
6.4 Follow change control processes and procedures f or all changes to system components.	2	3	Merchant change control records should be maintained for all changes to the encryption solution. In particular, diagrams must be kept current. For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems with custom applications that use the HPE SecureData Host SDK. Systems in the decryption environment are subject to change control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
6.5 Address common coding vulnerabilities in software-development processes.	1	3	For merchant-managed solutions, CHD encrypted at POI is decrypted within the merchant's CDE on decryption host systems with custom applications that use the HPE SecureData Host SDK. These applications are subject to all secure software lifecycle controls.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.	**1**	**1**	N/A
Implement strong access control measures			
Requirement 7: Restrict access to CHD by business need to know			Because there is no CHD in the merchant's environment, the scope of this requirement is dramatically reduced.
7.1 Limit access to system components and CHD to only those individuals whose job requires such access.	**1**	**3**	For merchant-managed environments, access control requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
7.2 Establish an access control system(s) for system components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**1**	**3**	For merchant-managed environments, access control requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
7.3 Ensure that security policies and operational procedures for restricting access to CHD are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
Requirement 8: Identify and authenticate access to system components			Because there is no CHD in the merchant's environment, the scope of this requirement is dramatically reduced.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	1	3	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.	1	3	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multifactor authentication.	1	3	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.4 Document and communicate authentication policies and procedures to all users.	1	3	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods.	1	3	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smartcards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**1**	**3**	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.7 All access to any database containing CHD (including access by applications, administrators, and all other users) is restricted.	**1**	**3**	For merchant-managed environments, identity and authentication requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
Requirement 9: Restrict physical access to CHD			This requirement does not apply to HPE SecureData Payments, but there are no requirements for physical access to CHD within HPE SecureData Payments, and nothing that would make a vendor non-compliant with PCI DSS Requirement 9.
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the CDE.	**1**	**3**	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
9.2 Develop procedures to easily distinguish between onsite personnel and visitors.	1	3	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.3 Control physical access for onsite personnel to sensitive areas.	1	3	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	1	3	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.5 Physically secure all media.	1	3	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	1	3	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
9.7 Maintain strict control over the storage and accessibility of media.	**1**	**3**	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	**1**	**3**	For merchant-managed environments, physical access requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	**3**	**3**	Merchant inspection of devices is applicable. The encryption solution provider may have additional inspection procedures that are required of the merchant.
9.10 Ensure that security policies and operational procedures for restricting physical access to CHD are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
Regularly monitor and test networks			
Requirement 10: Track and monitor all access to network resources and CHD			This does not apply to HPE SecureData Payments, but there is nothing within HPE SecureData Payments that would make a vendor non-compliant with PCI DSS Requirement 10.
10.1 Implement audit trails to link all access to system components to each individual user.	1	3	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
10.2 Implement automated audit trails for all system components to reconstruct the following events:	1	3	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
10.3 Record at least the following audit trail entries for all system components for each event:	1	3	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	1	3	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
10.5 Secure audit trails so they cannot be altered.	**1**	**3**	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	**1**	**3**	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**1**	**3**	For merchant-managed environments, logging and monitoring requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and CHD are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
Requirement 11: Regularly test security systems and processes			
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	**1**	**3**	For merchant-managed environments, regular testing requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	**1**	**3**	For merchant-managed environments, regular testing requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
11.3 Implement a methodology for penetration testing.	**1**	**3**	For merchant-managed environments, regular testing requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of and critical points in the CDE, and alert personnel to suspected compromises.	**1**	**3**	For merchant-managed environments, regular testing requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply to POS networks if appropriate separation of duties is implemented to protect encryption keys.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	**2**	**3**	For service provider solutions, (11.5.1) notifications from the encryption solution provider must be responded to in a timely manner. For merchant-managed environments, change detection requirements are applicable to protect the decryption host, HPE SecureData Appliance, HSM, and network devices providing network access control. Even in that case, this control will not apply t o POS networks if appropriate separation of duties is implemented to protect encryption keys.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	**3**	**3**	Requirements concerning policies are always applicable.
Maintain an information security policy			
Requirement 12: Maintain a policy that addresses information security for all personnel			This is not addressed by HPE SecureData Payments, but there is nothing within HPE SecureData Payments that would make a vendor non-compliant with PCI DSS Requirement 12.
12.1 Establish, publish, maintain, and disseminate a security policy.	**3**	**3**	Requirements concerning policies are always applicable.
12.2 Implement a risk-assessment process.	**3**	**3**	
12.3 Develop usage policies for critical technologies and define proper use of these technologies.	**3**	**3**	The merchant's critical technology policy should specify that only technologies specified by the encryption solution provider are used for card-present payments.

PCI DSS requirement	Solution provider managed decryption	Merchant managed	Assessor comments
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**3**	**3**	N/A
12.6 Implement a formal security awareness program to make all personnel aware of the importance of CHD security.	**3**	**3**	It is critical that merchants ensure employees are aware of both general CHD security and operation of the encryption solution according to provider instructions.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.	**1**	**3**	For merchant-managed environments, developers and administrators of the decryption environment have access to keys and decrypted credit card data and are therefore subject to this control.
12.8 Maintain and implement policies and procedures to manage service providers with whom CHD is shared, or that could affect the security of CHD.	**3**	**3**	Merchants must carefully manage the encryption solution provider.
12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of CHD the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.	**1**	**1**	N/A
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**3**	**3**	Notifications from the encryption solution provider must be responded to in accordance with their incident response plan.
12.11: Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.	**N/A**	**3**	Service providers must always meet this requirement.

Learn more at

voltage.com

hpe.com/software/datasecurity

ABOUT COALFIRE

As a trusted advisor and leader in cybersecurity, Coalfire has more than 15 years in IT security services. We empower organizations to reduce risk and simplify compliance, while minimizing business disruptions. Our professionals are renowned for their technical expertise and unbiased assessments and advice. We recommend solutions to meet each client's specific challenges and build long-term strategies that can help them identify, prevent, respond, and recover from security breaches and data theft. Coalfire has offices throughout the United States and Europe. **www.coalfire.com**

WP_HPE-SecureData-Payments_110716