WHITE PAPER

HPE SECUREDATA MOBILE PCI DSS TECHNICAL ASSESSMENT

TIM WINSTON | PCI/P2PE PRACTICE DIRECTOR

KEVIN MCDERMOTT | SECURITY CONSULTANT, COALFIRE LABS

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) and Payment Application – Qualified Security Assessor (PA-QSA) company to conduct an independent technical assessment of its HPE SecureData Mobile solution. Coalfire conducted technical testing activities for this assessment.

In this paper, Coalfire will describe the HPE SecureData Mobile solution and the particular requirements it addresses within PCI Data Security Standard (DSS) scope.

ABOUT HPE SECUREDATA MOBILE

HPE SecureData Mobile is intended to increase the security of mobile application platforms without impacting the buyer's experience and reduce merchant PCI scope by encrypting consumer cardholder data (CHD) in the application before it is submitted for authorization processing. HPE SecureData Mobile leverages HPE's key management architecture and allows mobile application merchants to integrate data encryption into checkout pages.

HPE SecureData Mobile encrypts data within the user's mobile application. The encryption keys come from a host outside of the merchant's environment. This means that a proper implementation of HPE SecureData Mobile protects all sensitive CHD from the moment that it is entered until decryption in the merchant's or service provider's data center. The mobile applications do not store unencrypted sensitive credit card data at any time, and dramatically reduce risk and applicable controls in PCI DSS scope over applications that rely on SSL/TLS transport security alone.

AUDIENCE

This assessment white paper has three target audiences:

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

ASSESSMENT SCOPE

HPE contracted with Coalfire to provide an independent technical security review of the HPE SecureData Mobile solution. The intent of this technical assessment was to analyze the impact on PCI DSS scope for merchants and service providers who implement HPE SecureData Mobile for their mobile applications.

METHODOLOGY

Coalfire has implemented industry best practices in its assessment and testing methodologies. Coalfire completed a multifaceted technical assessment process during the course of this project using these industry and audit best practices. Coalfire conducted technical lab testing in its Colorado lab on January 15, 2016.

At a high level, testing consisted of the following tasks:

1. Technical review of the provided HPE SecureData Mobile SDK
2. Evaluation of the data in-transit on the system running a demo mobile application using HPE SecureData Mobile

EXECUTIVE SUMMARY OF FINDINGS

HPE SecureData Mobile impacts PCI DSS compliance in two areas:

1. The mobile application
2. The trusted host environment

PCI DSS relevance to mobile applications depends on the technical implementation and use of the mobile device with the installed application. Refer to PCI Security Standards Council guidance:

- At A Glance: Applications Eligible for PA-DSS Validation (https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf)
- Mobile Payment Acceptance Applications and PA-DSS Frequently Asked Questions (https://www.pcisecuritystandards.org/documents/pa-dss_mobile_apps-faqs.pdf)

There are three broad scenarios for mobile applications:

1. Applications installed by consumers on their own devices do not impact merchant or service provider DSS compliance. As with web browsers, consumers accept the responsibility for their own devices. Merchants and service providers are responsible for the trusted host environment.
2. Applications that are part of a packaged service provider solution can be validated for Payment Application Data Security Standard (PA-DSS).
3. Applications that are packaged by the merchant for a point-of-sale (POS) solution are subject to merchant DSS assessment just like other customer POS systems.

This paper will address the PCI DSS impact of the first scenario, mobile applications installed on consumer devices, because it represents the majority of mobile applications. If you do not use a mobile application in this scenario, you should consult with a PCI QSA experienced with assessing mobile solutions to ensure proper PCI DSS compliance impact for a specific implementation.

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

- A properly designed and deployed HPE SecureData Mobile integrated mobile application has an impact on the assessment of **15 of PCI's 242 requirements, or 94%,** for the DMZ web services server in the trusted host environment.
- HPE SecureData Mobile reduces the risk of consumer CHD compromise and removes exposure of plain-text CHD to the mobile device or transmission to the trusted host environment by encrypting CHD in the mobile application immediately on entry.
- Merchants maintaining their own trusted host environment are still subject to all PCI DSS controls. However, most controls will apply to the secure web services host, HPE SecureData Key Management Server, hardware security modules (HSMs), and network devices providing network access control to that environment. The majority of controls (**up to 94%**) will not apply to DMZ web services servers 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 mobile commerce environment to a handful of centrally located systems.
- QSAs and acquiring banks may make a risk-based determination to completely remove the merchant mobile commerce 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.

Implementing a HPE SecureData Mobile solution should not lower a merchant's level of sensitivity to the security of their mobile applications environment. Merchants have the responsibility to implement security best practices for their servers and network regardless of PCI DSS scope reduction

ABOUT HPE SECUREDATA MOBILE

HPE SecureData Payments has three components:

1. Mobile application using the HPE SecureData Mobile SDK
2. HPE SecureData Key Management Server, which manages the mobile application activation and encryption key distribution that comprise the trusted host environment
3. Web services server using HPE SecureData Host SDK for data decryption

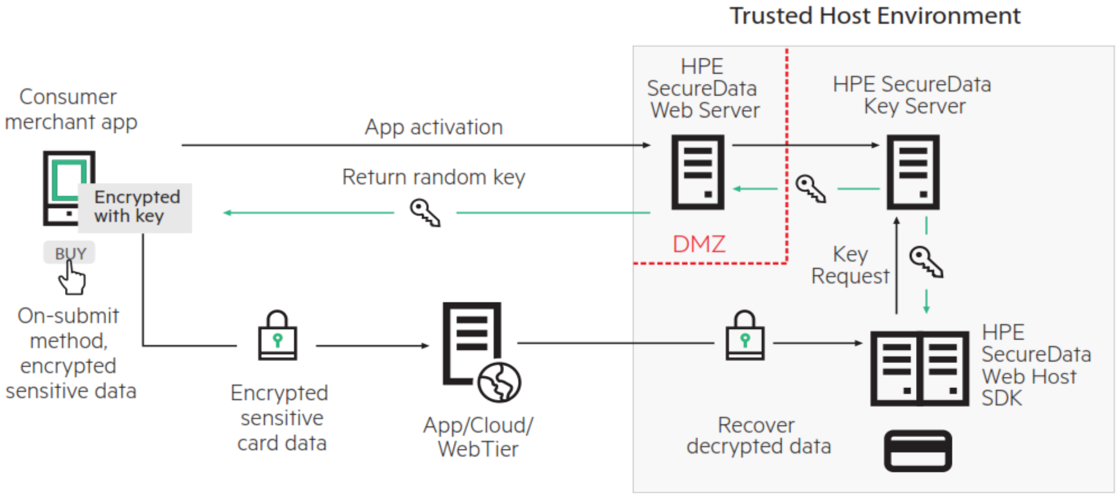

Figure 1: HPE SecureData Mobile components

For comparison, typical mobile applications do not encrypt data except for transport over the Internet between the mobile application and the DMZ web services server of the service provider. This leaves data exposed at three critical points:

1. On the device to other applications including malware
2. On the Internet to man-in-the-middle attacks, such as SSL Strip or BEAST
3. On the mobile service DMZ after the termination of the TLS/SSL tunnel

This impacts not only the security of payment data, but increases the number of systems subject to PCI DSS compliance. Any system that stores, processes, or transmits credit card data is subject to PCI DSS. In a typical scenario this would include the load balancers that terminate the TLS/SSL tunnel and all systems connected to networks on the path of data to the trusted host environment.

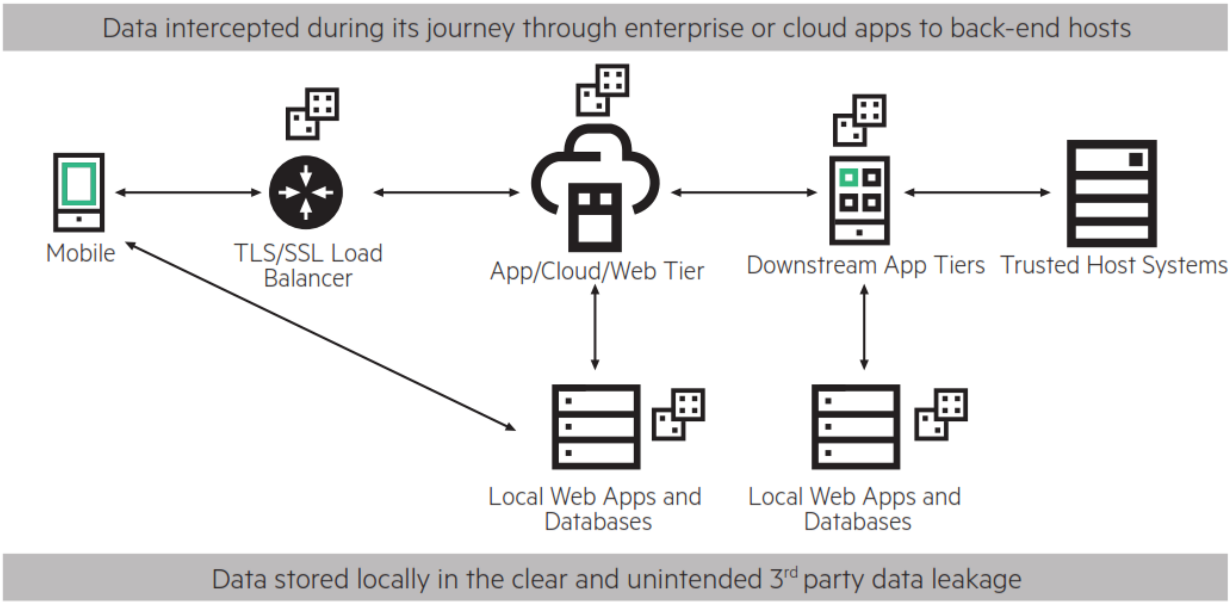
Data intercepted during its journey through enterprise or cloud apps to back-end hosts
Mobile
TLS/SSL Load Balancer
App/Cloud/Web Tier
Downstream App Tiers
Trusted Host Systems
Local Web Apps and Databases
Local Web Apps and Databases
Data stored locally in the clear and unintended 3rd party data leakage

Figure 2: Typical mobile application components

PCI DSS IMPACT

OVERVIEW

The benefits of using the HPE SecureData Mobile solution are two-fold:

1. A properly configured implementation using HPE SecureData Mobile could completely remove the merchant's mobile application from the scope of PCI DSS, if they are using a service provider for key management and data encryption.
2. Should a QSA decide that the merchant's mobile application system must remain in scope, HPE SecureData Mobile substantially reduces the impact of 94% of the PCI DSS requirements for DMZ web services servers.

MERCHANT PCI COMPLIANCE SCOPE AND CHD ENVIRONMENT

PCI compliance of mobile applications is addressed on the PCI website in the *Mobile Payment Acceptance Applications and PA-DSS Frequently Asked Questions* (https://www.pcisecuritystandards.org/documents/pa-dss_mobile_apps-faqs.pdf). Mobile applications are impacted by PCI DSS much differently than other web e-commerce and traditional payment software:

- Mobile applications for consumer use are not subject PCI DSS. While it is important to secure sensitive data from mobile applications, there are no PCI DSS compliance requirements that govern the application on consumer devices.
- Mobile applications that run on PCI PIN Transaction Security (PTS) approved mobile devices or purpose built mobile devices or integrated bundles may be validated under the PCI PA-DSS program and listed on the PCI website. Merchants using these solutions are responsible for following the implementation guide for the solution.
- Merchant managed mobile solutions are subject to all PCI DSS controls, similar to other POS systems. If unencrypted CHD is stored, processed, or transmitted by the device, it is subject DSS controls. This applies even if acquired sensitive data is immediately encrypted.

The most common scenario is the consumer application. The analysis below addresses only that scenario.

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 CHD. To reduce the scope of PCI DSS compliance requirements, a merchant can segment its network to separate the systems that store, transmit, or process CHD from those that do not. This method removes systems that are unrelated to payment card processing from PCI DSS scope.

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 secure cryptographic devices (SCDs) used for key management

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

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

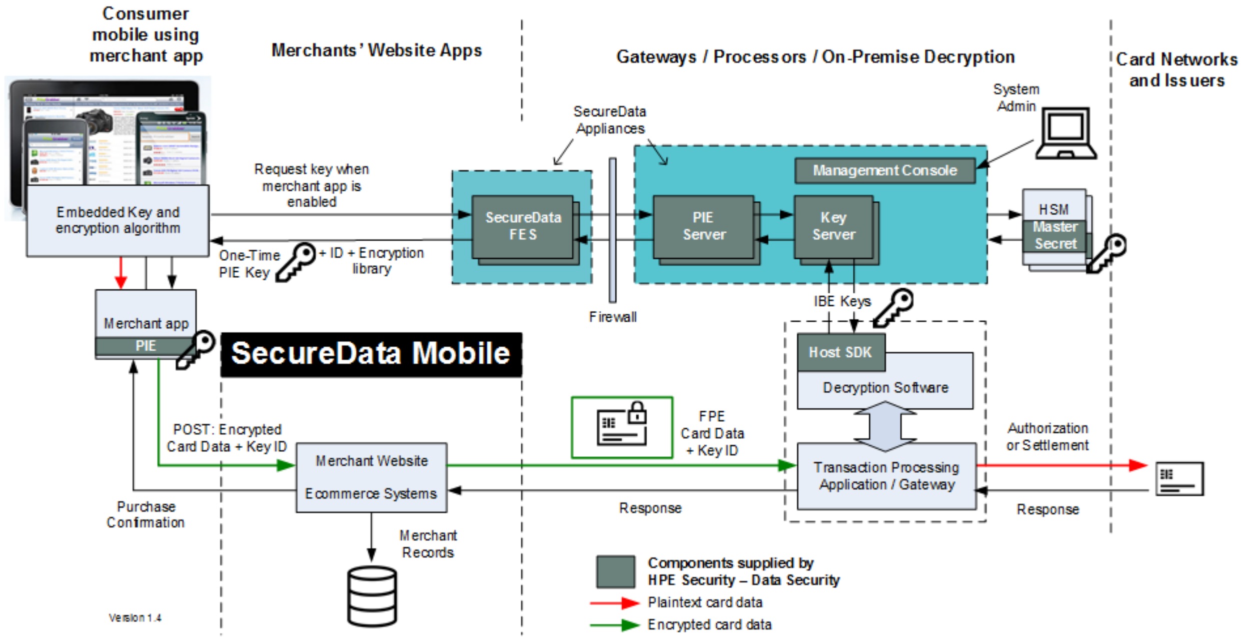

Figure 3: Key Architecture

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 depend on whether the merchant is using an HPE SecureData Mobile solution from a service provider or maintaining their own solution.

Legend:

🟠 Merchant is using a service provider managed e-commerce encryption

🔵 Merchant manages e-commerce payment encryption solution

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 Mobile. 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 Mobile solution, and will probably still be applicable during a PCI DSS 3.2 audit.

PCI DSS requirement	Solution provider managed	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 Mobile. Regardless, nothing within HPE SecureData Mobile prevents a vendor from using a properly configured firewall. HPE SecureData Mobile uses only standard communications protocols and ports.
1.3 Prohibit direct public access between the Internet and any system component in the CDE.	1	2	In a properly configured HPE SecureData Mobile solution, there is no CDE in the merchant’s environment.
1.3.4 Do not allow unauthorized outbound traffic from the CDE to the Internet	1	2	In a properly configured HPE SecureData Mobile solution, there is no CDE in the merchant’s environment.
1.3.6 Place system components that store CHD (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	1	2	In a properly configured HPE SecureData Mobile solution, there is no CDE in the merchant’s environment.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			HPE SecureData Mobile dramatically reduces the scope of this requirement, because so much of the merchant’s network can be put out of scope of PCI DSS.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	2	3	The applicable controls for this requirement can be significantly reduced because almost all merchant devices, servers, and workstations can be removed from testing as they do not process or store CHD, and this control does not apply to them. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
2.1.1 For wireless environments connected to the CDE or transmitting CHD, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and simple network management protocol (SNMP) community strings.	1	2	In a properly configured HPE SecureData Mobile solution, there is no CDE in the merchant's environment, and the merchant does not have CHD to transmit. Therefore, there is no possibility for a wireless environment to be connected to the CDE nor transmitting CHD.
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.	2	3	The applicable controls for this requirement can be significantly reduced because almost all merchant devices, servers, and workstations can be removed from testing as they do not process or store CHD and this control does not apply to them. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	2	3	Applies to perimeter network systems only for solution provider managed. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	2	3	Applies to perimeter network systems only for solution provider managed. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
2.2.4 Configure system security parameters to prevent misuse.	2	3	Applies to perimeter network systems only for solution provider managed. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2**	**3**	Applies to perimeter network systems only for solution provider managed. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
2.3 Encrypt all non-console administrative access using strong cryptography.	**2**	**3**	Applies to perimeter network systems only for solution provider managed. However, this requirement will still apply to perimeter firewalls/IDS/routers/wireless in the merchant environment.
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 that include at least the following for all CHD storage.	**1**	**3**	A properly configured HPE SecureData Mobile deployment will never store any CHD at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	**1**	**3**	A properly configured HPE SecureData Mobile deployment will not store any sensitive authentication data (SAD) data at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization.	**1**	**3**	A properly configured HPE SecureData Mobile deployment will not have access to full track data at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	1	3	A properly configured HPE SecureData Mobile deployment will not have access to card verification value (CVV) data at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	1	3	A properly configured HPE SecureData Mobile deployment will not have access to PIN block data at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.3 Mask primary account number (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	A properly configured HPE SecureData Mobile deployment will only have access to encrypted PAN that it cannot decrypt. Therefore, full PAN cannot display it at any time. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).	1	3	In a properly configured HPE SecureData Mobile deployment, every instance of PAN within the merchant's network is encrypted, and cannot be decrypted by the merchant. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	1	3	In a properly configured HPE SecureData Mobile service provider deployment, there is no CHD to encrypt in any way. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
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 of HPE SecureData Mobile. However, this requirement is partially covered because the merchant does not have access to the encryption keys at all. For merchant-managed solutions, these controls are critical. No one may be permitted access to both encrypted data and encryption keys. Strong split responsibility and dual control must be implemented for key management technology and processes to obtain any DSS compliance reduction.
3.5. Restrict access to cryptographic keys to the fewest number of custodians necessary.	1	3	HPE SecureData Mobile uses dynamically generated keys, and therefore has no key custodians for solution provider managed solutions. For merchant-managed solutions, this is control is supported by the key manager.
3.5.3 Store secret and private keys used to encrypt/decrypt CHD.	1	3	In a properly configured HPE SecureData Mobile deployment, the merchant has no access to encryption keys, and is not responsible for storing them. For merchant-managed solutions, this is control is supported by the key manager.
3.5.4 Store cryptographic keys in the fewest possible locations.	1	3	In a properly configured HPE SecureData Mobile deployment, the merchant has no access to encryption keys. For merchant-managed solutions, this is control is supported by the key manager.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of CDH	2	3	Because this requirement is about documentation, it lies outside of HPE SecureData Mobile. However, this requirement is partially covered because the merchant does not have access to the encryption keys at all. For merchant-managed solutions, merchants should follow HPE recommended procedures.
3.6.1 Generation of strong cryptographic keys	1	2	HPE SecureData Mobile generates strong cryptographic keys. For merchant-managed solutions, this control is supported by the key manager.
3.6.2 Secure cryptographic key distribution	1	2	HPE SecureData Mobile securely distributes cryptographic keys using TLS v. 1.2 For merchant-managed solutions, this control is supported by the key manager.
3.6.3 Secure cryptographic key storage	1	2	HPE SecureData Mobile securely stores cryptographic keys, and does so outside of the merchant's network. For merchantmanaged solutions, this control is supported by the key manager.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod	1	2	HPE SecureData Mobile dynamically generates a new key for each transaction.
3.6.5 Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised	1	2	HPE SecureData Mobile dynamically generates a new key for each transaction. For merchantmanaged solutions, this control is supported by the key manager.
3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control.	1	1	HPE SecureData Mobile has no manual key management operations.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
3.6.7 Prevention of unauthorized substitution of cryptographic keys	1	2	HPE SecureData Mobile programmatically generates keys and distributes them in a secure fashion using TLS v.1.2. For merchant-managed solutions, this is control is supported by the key manager.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities	1	3	HPE SecureData Mobile has no key custodians for solution provider managed solutions. For merchant-managed solutions, merchants should follow HPE recommended procedures.
3.7 Ensure that security policies and operational procedures for protecting stored CHD are documented, in use, and known to all affected parties.	2	3	Because this requirement is about documentation, it lies outside of SecureData Mobile. However, this requirement is partially covered because the merchant does not have access to any CHD data at any time, and so cannot store any. For merchant-managed solutions, merchants should follow HPE recommended procedures.
Requirement 4: Encrypt transmission of CHD across open, public networks			
4.1 Use strong cryptography and security protocols to safeguard sensitive CHD during transmission over open, public networks.	1	3	HPE SecureData Mobile uses TLS 1.2 for transmission over open networks. However, this transmission is done entirely externally to the merchant's network. For merchant-managed solutions, post-decryption data must be protected.
4.1.1 Ensure wireless networks transmitting CHD or connected to the CDE, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	1	3	There is neither a CDE, nor any CHD, within the merchant's environment for solution provider managed. Therefore, a wireless network cannot transmit CHD. For merchant-managed solutions, post-decryption data must be protected.
4.2 Never send unprotected PANs by end-user messaging technologies.	1	3	In a properly configured HPE SecureData Mobile deployment, the merchant has no access to unprotected PANs at all. For merchant-managed solutions, post-decryption data must be protected.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
4.3 Ensure that security policies and operational procedures for encrypting transmissions of CHD are documented, in use, and known to all affected parties.	2	3	Because this requirement is about documentation, it lies outside of HPE SecureData Mobile. However, this requirement is trivial because the merchant does not have any access to CHD. For merchant-managed solutions, post-decryption data must be protected.
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 Mobile, but there is nothing within HPE SecureData Mobile that would prevent an antivirus program from running properly. A vendor can fulfill PCI DSS Requirement 5 while properly implementing an HPE SecureData Mobile solution.
5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	2	3	Only perimeter firewalls and the web services server are in scope. However, it is recommended to follow industry best practices and deploy antivirus on all systems. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
5.1.1 Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.	2	3	Only perimeter firewalls and the web services server are in scope. However, it is recommended to follow industry best practices and deploy antivirus on all systems. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
5.2 Ensure that all antivirus mechanisms are maintained.	2	3	Only perimeter firewalls and the web services server are in scope. However, it is recommended to follow industry best practices and deploy antivirus on all systems. For merchant-managed solutions, all systems that store, process, or transmit decrypted are subject to this control.
Requirement 6: Develop and maintain secure systems and applications			This requirement is extremely important, because HPE SecureData Mobile requires an application to be built using the HPE SecureData Mobile. HPE itself meets all of the standards required by this requirement, so using HPE SecureData Mobile would not make a vendor non-compliant with PCI DSS Requirement 6.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
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**	This control must be maintained for any systems that can impact the security of CHD or the integrity of the implementation of HPE SecureData Mobile.
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**	This control must be maintained for any systems that can impact the security of CHD or the integrity of the implementation of HPE SecureData Mobile.
6.3 Develop internal and external software applications (including mobile-based administrative access to applications) securely.	**2**	**3**	A properly implemented solution using HPE SecureData Mobile forces the developer to use industry standards and best practices, and to incorporate information security throughout the software development lifecycle, simply because of the design of the solution.
6.5 Address common coding vulnerabilities in software-development processes as follows: Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. Develop applications based on secure coding guidelines**.**	**1**	**1**	While applications should always be developed securely and vulnerability tested, using HPE SecureData Mobile eliminates PCI DSS compliance for reporting for mobile applications properly implementing the solution.

PCI DSS requirement	Solution provider managed	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 by either one of the following methods: Reviewing public-facing web applications via manual or by automated application vulnerability security assessment tools or methods, at least annually and after any changes.	1	1	Web service interfaces are not web applications. They are not subject to vulnerabilities common to web applications. Therefore, this requirement does not apply.
Implement strong access control measures			
Requirement 7: Restrict access to 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.	2	3	There is no CHD in the merchant's environment in the case of solution provider managed solutions, so that portion of the requirement is irrelevant. Additionally, the scope of this requirement is reduced to perimeter systems and the web application server. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources	2	3	See 7.1
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	2	3	See 7.1
7.1.3 Assign access based on individual personnel's job classification and function.	2	3	See 7.1

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
7.1.4 Require documented approval by authorized parties specifying required privileges.	2	3	See 7.1
7.2 Establish an access control system(s) for systems components that restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed.	2	3	The scope of this requirement is reduced to perimeter systems and the web application server. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
7.2.1 Coverage of all system components	2	3	See 7.2
7.2.2 Assignment of privileges to individuals based on job classification and function	2	3	See 7.2
7.2.3 Default "deny-all" setting	2	3	See 7.2
7.3 Ensure that security policies and operational procedures for restricting access to CHD are documented, in use, and known to all affected parties.	2	3	The scope of this requirement is reduced to perimeter systems and the web application server. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
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.
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.	2	3	The applicable controls should only apply to perimeter network systems and the web application server. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
8.1.1 Assign all users a unique ID before allowing them to access system components or CHD.	2	3	See 8.1

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**2**	**3**	See 8.1
8.1.3 Immediately revoke access for any terminated users.	**2**	**3**	See 8.1
8.1.4 Remove/disable inactive user accounts within 90 days.	**2**	**3**	See 8.1
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access.	**2**	**3**	See 8.1
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**2**	**3**	See 8.1
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**2**	**3**	See 8.1
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**2**	**3**	See 8.1
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.	**2**	**3**	See 8.1
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	**2**	**3**	See 8.1

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	**2**	**3**	See 8.1
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	**2**	**3**	See 8.1
8.2.4 Change user passwords/passphrases at least once every 90 days.	**2**	**3**	See 8.1
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	**2**	**3**	See 8.1
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	**2**	**3**	See 8.1
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multifactor authentication.	**2**	**3**	See 8.1
8.4 Document and communicate authentication policies and procedures to all users.	**2**	**3**	See 8.1

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods.	**2**	**3**	See 8.1
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.	**2**	**3**	See 8.1
8.7 All access to any database containing CHD (including access by applications, administrators, and all other users) is restricted.	**2**	**3**	See 8.1
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	**2**	**3**	See 8.1
Requirement 9: Restrict physical access to CHD			This requirement does not apply to HPE SecureData Mobile, but there are no requirements for physical access to CHD within HPE SecureData Mobile, 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.	**2**	**3**	Since there is no CDE in the merchant's environment for solution provider managed solutions, this control does not apply. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	**2**	**3**	See 9.1
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	**2**	**3**	See 9.1
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**1**	**3**	See 9.1
9.3 Control physical access for onsite personnel to sensitive areas.	**2**	**3**	CHD is not accessible in the merchant location for solution provider managed solutions. Merchants should still ensure that there are basic training and procedures to ensure that unauthorized visitors cannot access perimeter systems. For merchant-managed solutions, these controls apply to the decryption environment.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	**2**	**3**	See 9.3
9.4.2 Visitors are identified and given a badge or other identification that expires and visibly distinguishes the visitors from onsite personnel.	**2**	**3**	See 9.3
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	**2**	**3**	See 9.3

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where CHD is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	**2**	**3**	See 9.3
9.5 Physically secure all media.	**1**	**3**	The merchant should not have access to any PAN, SAD, or CHD, which means that physical media is not required to be secured. For merchant managed solutions, these controls apply to the decryption environment.
9.5.1 Store media backups in a secure location, preferably an offsite facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	**1**	**3**	See 9.5
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**1**	**3**	See 9.5
9.6.1 Classify media so the sensitivity of the data can be determined.	**1**	**3**	See 9.5
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	**1**	**3**	See 9.5
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	**1**	**3**	See 9.5
9.7 Maintain strict control over the storage and accessibility of media.	**1**	**3**	See 9.5

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	1	3	See 9.5
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	1	3	See 9.5
9.8.1 Shred, incinerate, or pulp hardcopy materials so that CHD cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	1	3	See 9.5
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	1	1	There are no devices that capture payment card data via direct physical interaction in this solution.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	1	1	See 9.9
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	1	1	See 9.9
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices.	1	1	See 9.9

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
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.	**2**	**3**	This is a documentation requirement, but it is trivialized because SecureData Mobile does not have any access to CHD. For merchant-managed solutions, this control applies to the decryption environment.
Regularly monitor and test networks			
Requirement 10: Track and monitor all access to network resources and CHD			This does not apply to HPE SecureData Mobile, but there is nothing within HPE SecureData Mobile 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.	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**2**	**3**	See 10.1
10.2.1 All individual user accesses to CHD	**2**	**3**	See 10.1
10.2.3 Access to all audit trails	**2**	**3**	See 10.1
10.2.4 Invalid logical access attempts	**2**	**3**	See 10.1
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to, creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	**2**	**3**	See 10.1
10.2.6 Initialization, stopping, or pausing of the audit logs	**2**	**3**	See 10.1
10.2.7 Creation and deletion of system-level objects	**2**	**3**	See 10.1

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
10.3 Record at least the following audit trail entries for all system components for each event:	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
10.3.1 User identification	**2**	**3**	See 10.1
10.3.2 Type of event	**2**	**3**	See 10.1
10.3.3 Date and time	**2**	**3**	See 10.1
10.3.4 Success or failure indication	**2**	**3**	See 10.1
10.3.5 Origination of event	**2**	**3**	See 10.1
10.3.6 Identity or name of affected data, system component, or resource	**2**	**3**	See 10.1
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.	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
10.4.1 Critical systems have the correct and consistent time.	**2**	**3**	See 10.4
10.4.2 Time data is protected.	**2**	**3**	See 10.4
10.4.3 Time settings are received from industry-accepted time sources.	**2**	**3**	See 10.4
10.5 Secure audit trails so they cannot be altered.	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
10.5.1 Limit viewing of audit trails to those with a job-related need.	2	3	See 10.5
10.5.2 Protect audit trail files from unauthorized modifications.	2	3	See 10.5
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	2	3	See 10.5
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	2	3	See 10.5
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	2	3	See 10.5
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	2	3	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions	2	3	See 10.6

PCI DSS requirement	Solution provider managed	Merchant managed	Assessor comments
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	**2**	**3**	See 10.6
10.6.3 Follow up exceptions and anomalies identified during the review process.	**2**	**3**	See 10.6
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).	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
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.	**2**	**3**	For solution provider managed solutions, control applies to perimeter network systems only. For merchant-managed solutions, all systems that store, process, or transmit decrypted CHD are subject to this control.
Requirement 11: Regularly test security systems and processes			This is not addressed by HPE SecureData Mobile, but there is nothing within HPE SecureData Mobile that would make a vendor non-compliant with PCI DSS Requirement 11.
Maintain an information security policy			
Requirement 12: Maintain a policy that addresses information security for all personnel			This is not addressed by HPE SecureData Mobile, but there is nothing within HPE SecureData Mobile that would make a vendor non-compliant with PCI DSS Requirement 12.

TECHNICAL INFORMATION

NETWORK DIAGRAM

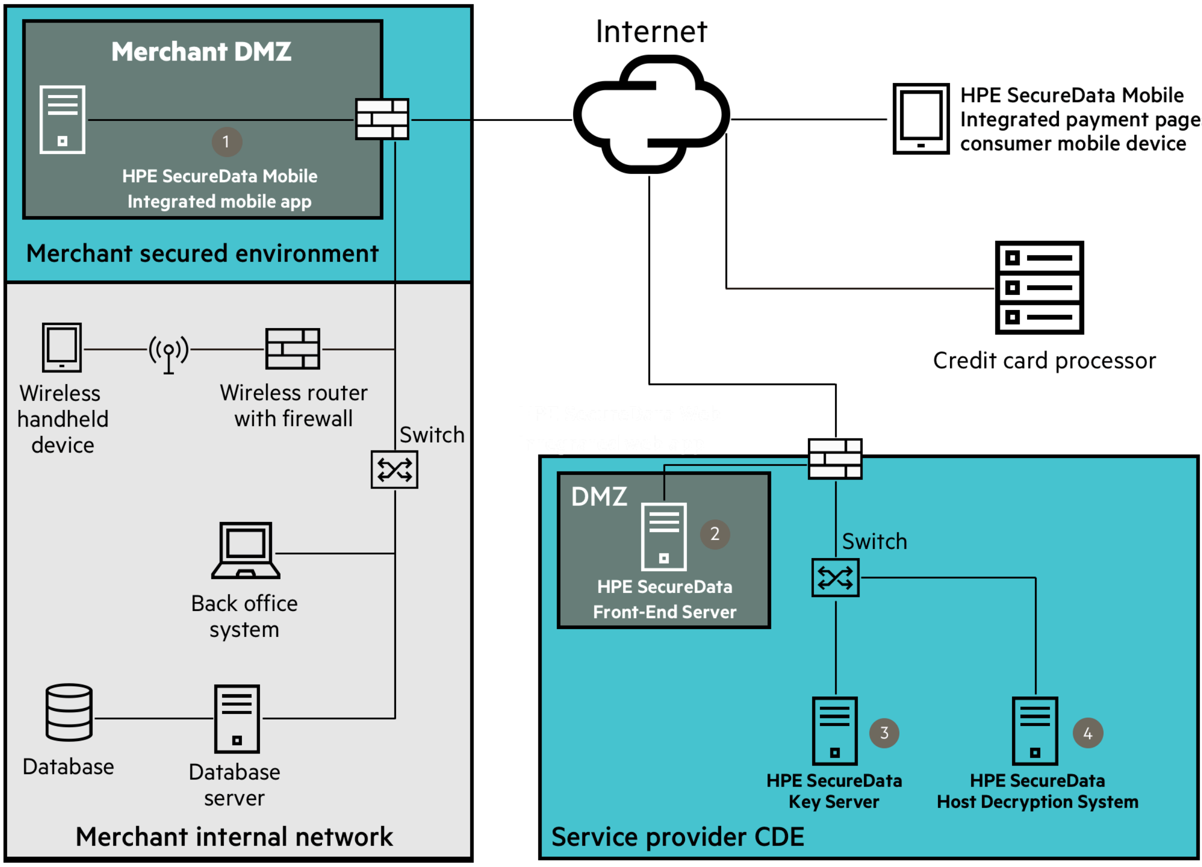

Figure 4: HPE SecureData Mobile deployment

Components

An HPE SecureData Mobile deployment consists of the following components:

1. **Merchant's mobile server**
2. **The HPE SecureData Front-End Server (FES),** which communicates with the web application and the key server
3. **The HPE SecureData Key Server (KS),** which services key requests from the FES and the HPE SecureData Host Decryption System
4. **The HPE SecureData Host Decryption System,** which is used by the host to decrypt the encrypted data

DATAFLOW DIAGRAM

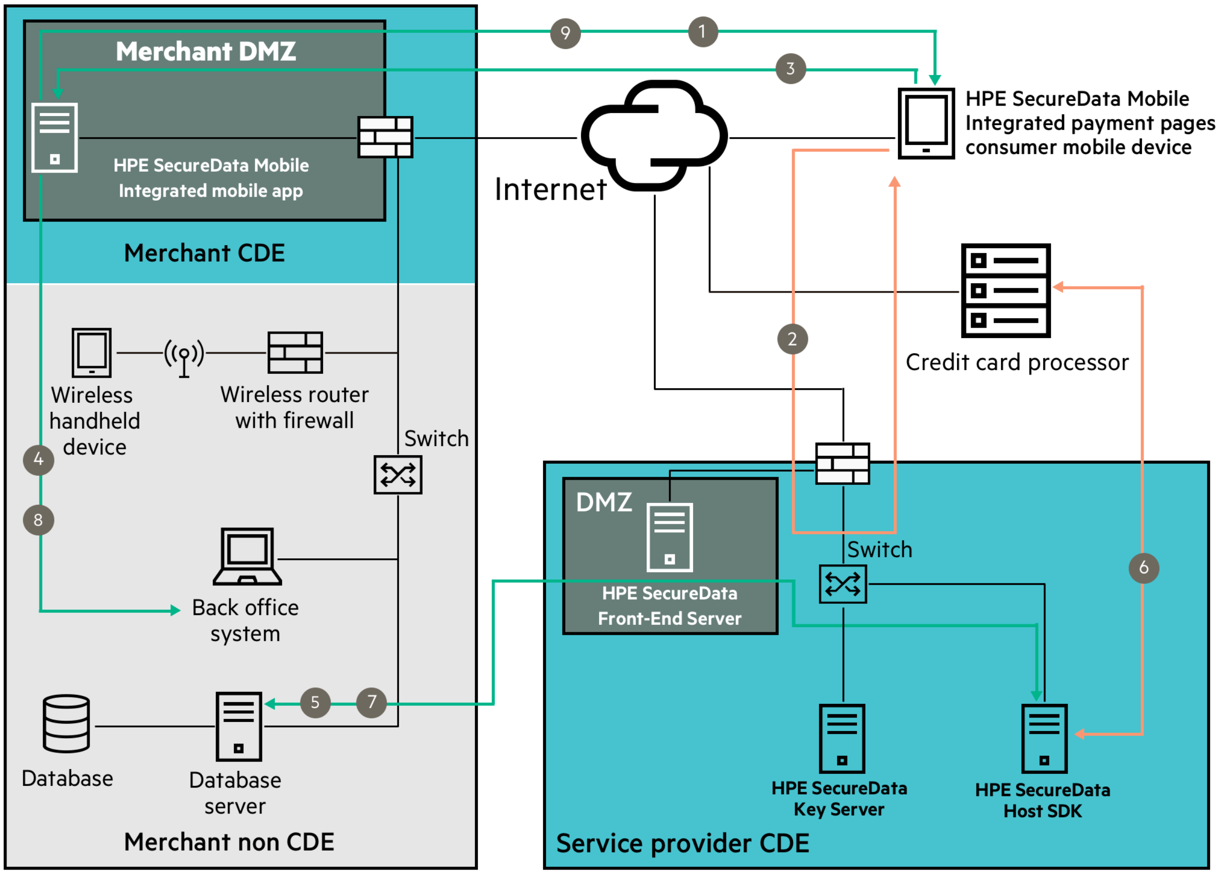

Figure 5: HPE SecureData Mobile dataflow example

Data flow

1. An HPE Page-Integrated Encryption (PIE) integrated merchant payment mobile application captures the cleartext payment data from the consumer mobile endpoint prior to the on-submit event.
2. A request is sent to the HPE SecureData FES that generates the encryption key and key ID specific to the transaction.
3. The customer enters their card data into their mobile application, and onsubmit triggers the call to encrypt the sensitive data using HPE SecureData Mobile libraries integrated into the merchant mobile application. This encrypted data is then posted to the merchant web server.
4. Encrypted card data can be sent through other merchant systems for storage and transactional recording. Because the merchant cannot decrypt this data, it is not considered CHD by PCI, and can be stored outside of the CDE.
5. Encrypted card data is submitted to the service provider for decryption and the authorization request.
6. Decrypted card data is submitted securely to the processor for authorization.
7. The authorization result (approved / denied) is returned to the merchant's network. No CHD is returned.
8. The authorization result (approved / denied) is returned to the merchant's web server. Again, no CHD is returned.
9. The authorization result (approved / denied) is returned to the consumer mobile endpoint. Again, no CHD is returned.

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-Mobile_110716