Hewlett Packard Enterprise | COALFIRE

HPE SecureData Web with Page-Integrated Encryption (PIE) Technology

Prepared for HPE Security—Data Security by:
Coalfire Systems Inc.
March 2, 2012

Technical white paper

Contents

Executive Summary

Overview

Merchants worldwide face the reality of breaches to their sensitive data due to inadequate security controls and vulnerable applications. Online merchants, in particular, are the targets of malicious individuals and organizations seeking to capture consumer cardholder data by exploiting common vulnerabilities in e-Commerce solutions.

Enterprise security and data protection firm HPE Security—Data Security has developed a data protection technology, referred to as HPE SecureData Web with HPE Page-Integrated Encryption (PIE) Technology, to protect sensitive consumer data entered via a consumer's browser. E-Commerce merchants now have an alternate approach for protecting sensitive data submitted during the e-Commerce checkout process, which can reduce the burden of merchant PCI DSS compliance.

HPE Security—Data Security contracted with leading independent security firm Coalfire Systems to provide a security review of the HPE SecureData Web with HPE PIE Technology solution. The intent of this project was to assess the security of the solution against industry best practices related to application security and data field encryption as well as analyze the impact on PCI DSS scope for merchants who implement it.

The HPE SecureData Web with HPE PIE Technology Solution

HPE SecureData Web with HPE PIE Technology solution is intended to increase the security of e-Commerce platforms without impacting the buyer's experience and reduce merchant PCI scope by encrypting consumer cardholder data in the browser before it is submitted for authorization processing. HPE PIE technology leverages HPE SecureData architecture and allows e-Commerce merchants to integrate data encryption into e-Commerce checkout pages without page redirection or the loss of brand identity.

HPE SecureData Web with HPE PIE Technology consists of the following components:

- The Merchant payment browser gets loaded with a javascript to encrypt the sensitive data entered by the consumer.
- The HPE SecureData Front-End Server (FES), which serves up the JavaScript files to the e-Commerce application.
- The HPE SecureData Key Server (KS), which services key requests from the FES and the HPE SecureData Host SDK.
- The HPE SecureData Host SDK used by the decrypting host to decrypt the encrypted data.

Summary of Key Findings

The key findings from Coalfire's security review of the HPE SecureData Web with HPE PIE Technology solution are:

- A properly designed and deployed HPE SecureData Web with HPE PIE Technology -integrated e-Commerce application:
  - Represents an attack surface and threat environment similar to that of a hosted payments page.
  - Reduces the risk of consumer cardholder data compromise and removes exposure of plain text cardholder data to the e-Commerce merchant by encrypting cardholder data in the consumer's browser.
  - Can significantly reduce PCI DSS scope and validation requirements similar to merchants implementing a hosted payments page solution.
- Acquiring banks and QSAs may make a risk-based determination to completely remove the merchant e-Commerce system from scope of PCI DSS, thereby further reducing the cost of validating PCI DSS compliance, in a way similar to a hosted payments page solution.
- Implementing a HPE SecureData Web with HPE PIE Technology—integrated e-Commerce solution or hosted payments page should not lower a merchant's level of sensitivity to the security of their e-Commerce environment. Merchants have the responsibility to implement security best practices for their web server and network regardless of PCI DSS scope reduction.

Detailed Project Overview

Merchants worldwide continue to face the reality of breaches to their sensitive data due to inadequate security controls and insecurely developed and deployed applications. Online merchants, in particular, are the targets of malicious users seeking to exploit common vulnerabilities in e-Commerce applications in order to capture consumer cardholder data.

HPE Page-Integrated Encryption (PIE), a new data protection technology, protects consumer personal data entered via the consumer's browser. Combined with HPE SecureData Web, an enterprise-class data protection architecture which implements the supporting components of HPE PIE technology, e-Commerce merchants now have an alternate approach for protecting consumer primary account number (PAN) and other sensitive data submitted during the e-Commerce checkout process, reducing the burden of PCI DSS on the merchant infrastructure. Such a solution can significantly reduce the scope and cost of PCI DSS compliance.

HPE Security—Data Security contracted with leading independent security governance, risk management and compliance (GRC) firm Coalfire Systems to provide a security review of the HPE SecureData Web with HPE PIE Technology solution. The intent of this technical assessment was to assess the security of the solution against industry best practices related to e-Commerce application security and data field encryption, as well as analyze the impact on PCI DSS scope for merchants and service providers who implement the components of this solution.

The primary purpose of the technical testing was to validate correct implementation of the HPE Format-Preserving Encryption employed by the HPE PIE technology and identify specific risks associated with the design and implementation of HPE SecureData Web in a merchant e-Commerce system. Additionally, Coalfire analyzed the typical deployment scenario to evaluate the potential for PCI DSS scope reduction for both merchants and service providers.

The HPE SecureData Web with HPE PIE Technology Overview

HPE SecureData Web with HPE PIE Technology provides data field encryption for web-based payment card transactions, with the intent to reduce risk of data compromise and a merchant's PCI DSS scope. HPE SecureData Web with HPE PIE Technology encrypts consumer cardholder data in the browser context before it is submitted to the merchant's payment/e-Commerce web server. To achieve integration into existing applications, HPE PIE technology is deployed into an e-Commerce application via simple Javascript. HPE PIE leverages existing HPE Format-Preserving Encryption (FPE), which is built on FFX mode AES with randomly generated single-use keys. This architecture allows e-Commerce merchants to integrate session based data encryption into e-Commerce checkout pages without page redirection or the loss of brand identity.

The components of the HPE SecureData Web with HPE PIE Technology in a typical deployment are illustrated below:

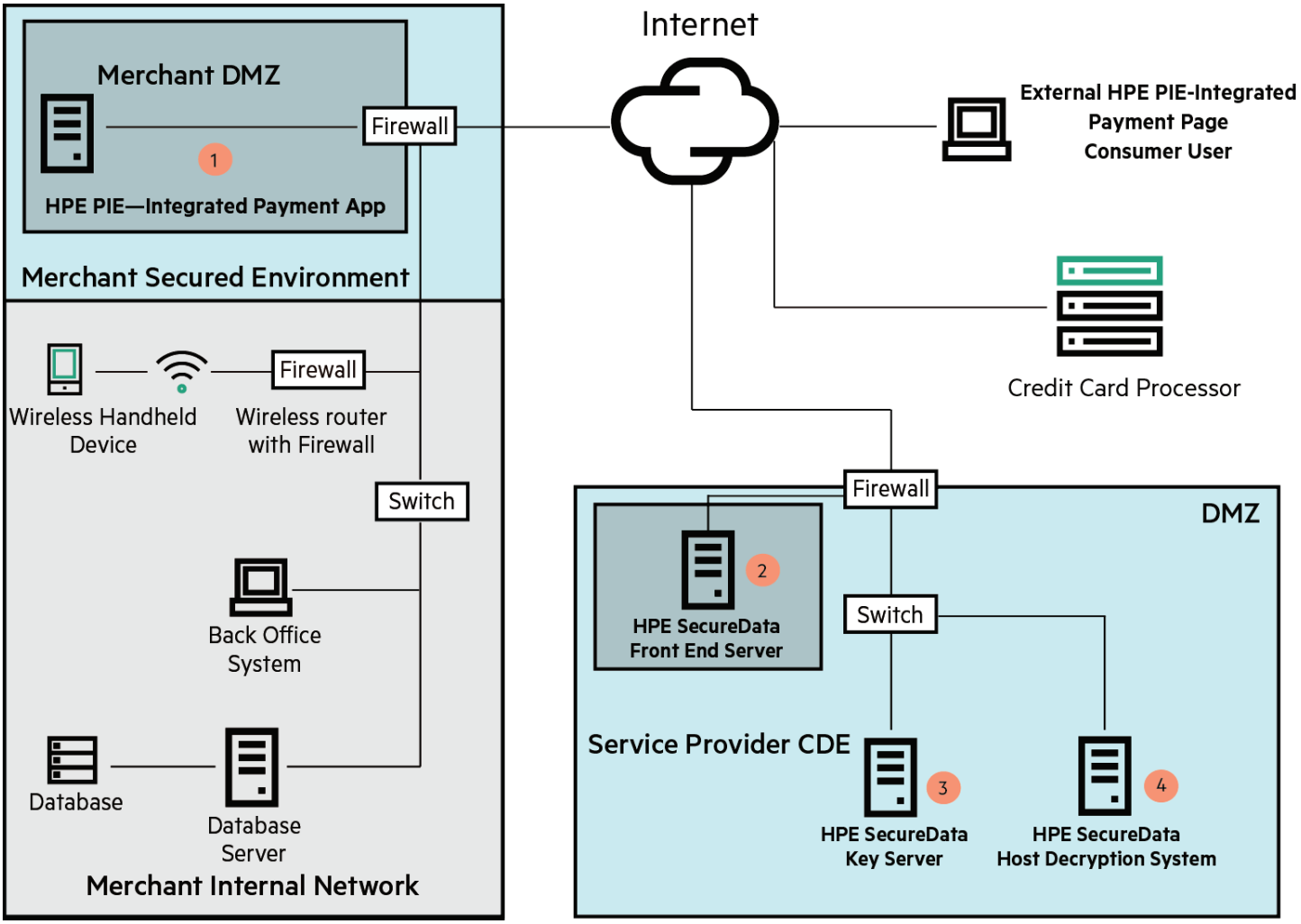

Figure 1. Typical Merchant Network with HPE SecureData Web Example

1. Merchant e-Commerce application: This application includes JavaScript files which contain dynamically generated, single-use cryptographic data and functions to encrypt consumer cardholder data entered via a browser form.
2. HPE SecureData Front-End Server (FES): This server provides static JavaScript files and dynamically-generated cryptographic data to HPE PIE technology-integrated payment pages.
3. HPE SecureData Key Server (KS): This server provides key management services to both the FES and the decryption environment (i.e. Host Decryption System) via the HPE SecureData Payments Host SDK.
4. HPE SecureData Host SDK: This is an API that can be integrated into a decryption host, appliance or HSM for decrypting encrypted data for subsequent clear text processing.

The HPE SecureData Web with HPE PIE Technology Operational Overview & Data Flow

In a typical deployment scenario, the merchant hosts the HPE PIE technology-integrated e-Commerce application and all backend components (i.e. HPE SecureData FES, HPE SecureData Key Server and HPE SecureData Host Decryption System) are hosted by a payment service provider (i.e. payment gateway or processor) as illustrated above in Figure 1. An alternate deployment scenario occurs when the merchant hosts all components, i.e. the e-Commerce application and all backend systems and services, in their network. The HPE SecureData Web with HPE PIE Technology infrastructure operates as follows:

1. When the merchant payment page loads into a consumer browser, two JavaScript files are loaded into the payment page from the HPE SecureData Front End Server (FES): **encryption.js**, a static file providing the encryption functions, and **getkey.js**, a dynamic file containing the AES key, the key ID, and various other parameters requested from the HPE SecureData Key Server (KS). The key and key ID are unique to every page load; the HPE SecureData FES requests a new key and key ID from the HPE SecureData Key Server (KS) every time **getkey.js** is loaded by a merchant payment page.
2. When the consumer has entered payment card data into the merchant payment form and clicked the "submit" button, the OnSubmit event triggers the HPE PIE JavaScript function to encrypt the cardholder data on the page before being submitted to the merchant web server. The encrypted cardholder data, along with the key ID, are transmitted to the merchant web server for subsequent authorization processing.
3. The encrypted cardholder data, along with the key ID, move through various servers on the Merchant network until it arrives at the decryption host running the HPE SecureData Host SDK, either in the hosted payment processor environment (Figure 1) or in the merchant-hosted decryption environment. The Decryption System via the HPE SecureData Host SDK requests the encryption key from the HPE SecureData KS using the key ID, and uses the provided key to decrypt the cardholder data for subsequent processing.

The following diagram (Figure 2) further illustrates how data flows through the system:

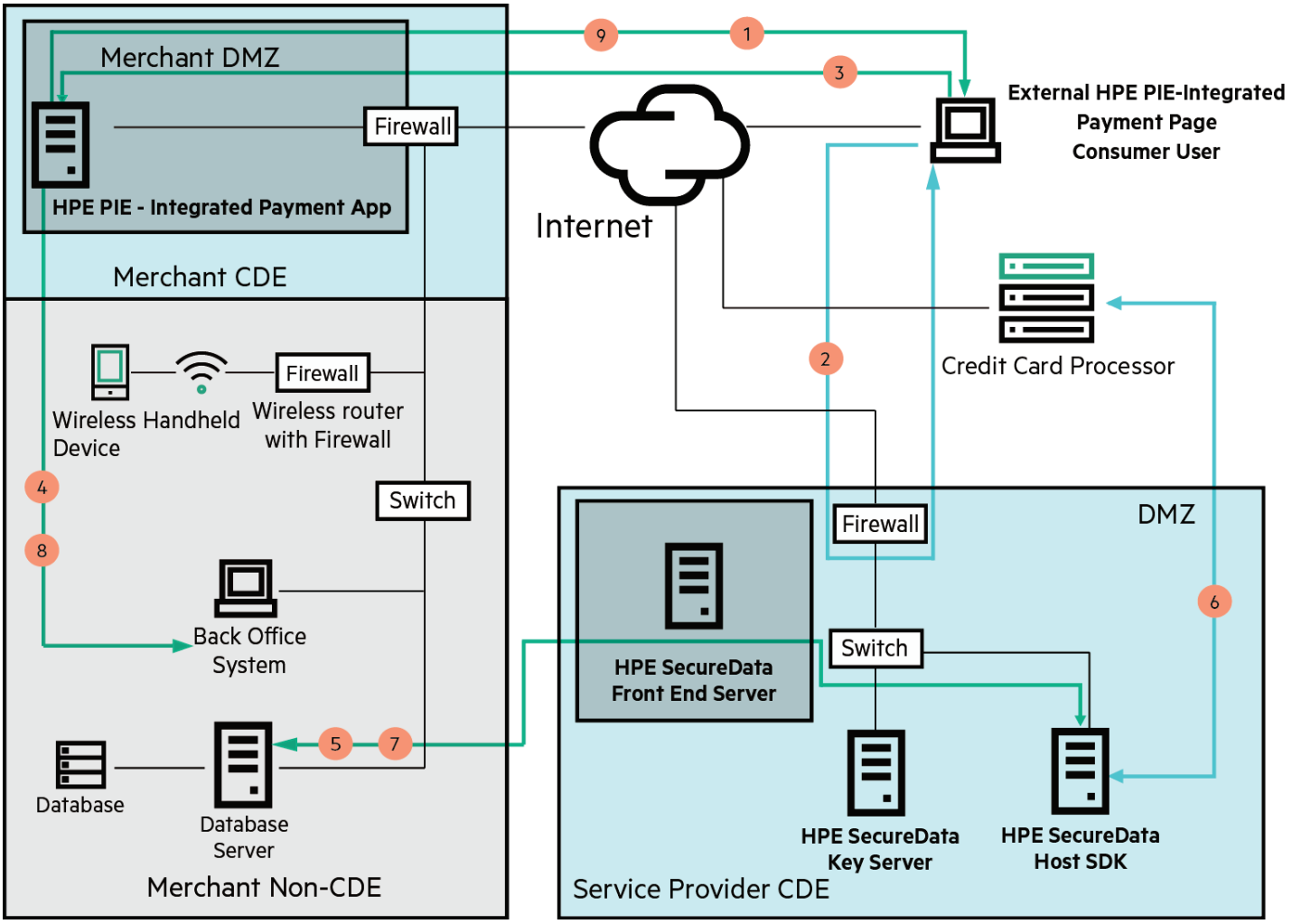

Figure 2. HPE SecureData Web Dataflow Example

1. Requested HPE PIE technology-integrated payment acceptance form sent to the end-user browser and captures cleartext data prior to OnSubmit event.
2. HPE PIE JavaScript files sent to browser. These files include a static file with encryption algorithm and dynamically generated file that contains the encryption key and key id for this transaction.
3. Card data entered into form and OnSubmit triggers JavaScript call to encrypt data using HPE PIE-included JavaScript functions and encryption key. Encrypted data posted to web server.
4. Encrypted card data may pass through other merchant systems for transactional recording.
5. Encrypted card data submitted to service provider for decryption and authorization request.
6. Decrypted card data is submitted over secure channel to processor for authorization.
7. Authorization result (approved/denied) is returned to the merchant network. No cardholder data.
8. Authorization result (approved/denied) is returned to the merchant web server. No cardholder data.
9. Authorization result (approved/denied) is returned to the end-user browser. No cardholder data.

Comparison of HPE SecureData Web with HPE PIE Technology to Hosted Payments Page

HPE SecureData Web with HPE PIE Technology represents a unique approach to protecting consumer cardholder data entered via e-Commerce applications. However, additional technology solutions exist in the market today to protect consumer cardholder data entering the payment processing stream through e-Commerce applications. The primary solution deployed to date is the hosted payments page. An e-Commerce application integrates to a hosted payments page by redirecting the consumer user from the merchant-hosted e-Commerce web server to a service provider-hosted payments page. An alternative to this deployment occurs when the merchant-hosted e-Commerce application integrates a hosted order form into its checkout page in an iFrame.

The following table provides a high-level comparison of HPE SecureData Web with HPE PIE Technology and the hosted payments page solution:

HPE SECUREDATA WEB WITH HPE PIE TECHNOLOGY	HOSTED PAYMENTS PAGE
E-Commerce Merchant hosts their e-Commerce system.	E-Commerce Merchant hosts their e-Commerce System.
Merchant e-Commerce system hosts the payment page, including order completion and checkout form(s) integrated with the HPE PIE technology.	Merchant e-Commerce system redirects to fully hosted payments page or integrates a fully hosted payments page into an iFrame.
Cardholder data is entered by a consumer via the merchant hosted, HPE PIE technology-integrated payment form.	Cardholder data is entered by a consumer via the fully hosted payment form.
Data field encryption occurs in the consumer browser via the onSubmit event handler. Transport layer encryption is also used between the browser and Merchant e-Commerce system.	Data field encryption does not typically occur in the hosted payments page solution. Transport layer encryption protects data in transit between the browser and processing back-end.
Encrypted cardholder data passes through the merchant network to the HPE SecureData Web back-end systems for decryption and authorization processing. Since the merchant has no access to symmetric encryption keys or the decryption process, this cardholder data may be considered out of scope of PCI (similar to how point-to-point-encrypted data is considered out of scope) and the systems through which this data passes can be considered out of scope of PCI DSS.	Cardholder data is posted to the payment page service provider back-end systems for authorization. No cardholder data (whether encrypted or in the clear) typically passes through the merchant network in a hosted payments page deployment, therefore these merchant systems can be considered out of scope of PCI DSS.
HPE SecureData Web back-end systems decrypt the cardholder data and push downstream for authorization processing.	Payment service provider is the end point for transport layer encryption and subsequent authorization processing using cleartext card data.
Authorization response is returned via the Merchant e-Commerce system to the consumer browser.	Authorization response is returned to the consumer browser by the hosted payments page service provider.

The comparison of these two solutions is important for the following reasons:

- Hosted payments pages have been available and deployed for some time and a common understanding exists of their impact on merchant PCI DSS compliance scope when properly deployed. Typically, the e-Commerce merchant's web server(s) and back-office system(s) in this type of payment processing infrastructure can be brought out of scope of PCI DSS since they do not capture, store, process or transmit cardholder data as part of authorization or settlement.
- E-Commerce applications integrated with hosted payments pages operate in a threat landscape very similar to a HPE SecureData Web with HPE PIE Technology—integrated e-Commerce application, i.e. exposure via the public internet to web application vulnerabilities. Both solutions operate in an environment where web application vulnerabilities may allow a malicious user to subvert security controls and allow access to consumer cardholder data in the clear.
- Hosted payments page solutions rely on the hosting Service Provider to provide security both for the hosted payments page and for the back-end infrastructure (i.e. servers supporting the hosted interface and payment processing functionality). These solutions also rely on the e-Commerce merchant to provide a proper and secure integration of their e-Commerce solution to the hosted payments page.

- HPE SecureData Web with HPE PIE Technology –integrated solutions rely on the HPE SecureData Web Service Provider (i.e. the host of the HPE SecureData FES, HPE SecureData KS and HPE SecureData Host Decryption System) to provide the security for the systems responsible for all key management and encryption/decryption functionality and access to cleartext cardholder data. These solutions rely on the e-Commerce merchant to provide a proper and secure design and implementation of their payment form and its integration to the HPE PIE technology interfaces and encryption functions.
- Both Visa and MasterCard recognize that hosted payments pages are not immune to compromise by vulnerable merchant e-Commerce web servers.

Visa recommends the following in their publication[1]:

- E-commerce merchants should ensure that regular checks of their website are carried out for any new or unknown web-pages or files. In particular, merchants should regularly check the code that redirects their customers to the third party hosted payments page is the same code that was provided to them by the third party and has not been modified.
- If the code that links to the hosted payments page is integrated into a merchant's shopping cart, e-commerce merchants should ensure that their shopping cart application is patched with the most up-to-date version available.
- E-commerce merchants should discuss security with their web hosting provider and ensure they have secured their systems appropriately. Web and database servers should be hardened to disable default settings and unnecessary services. Many international system hardening standards exist such as those provided by the center for Internet security—http://cisecurity.org/benchmarks.html and merchants should encourage their web host provider to adopt these standards.
- E-commerce merchants that utilize web hosting providers or third party payment providers that store, process and/or transmit cardholder data must maintain on-going compliance to the Payment Card Industry Data Security Standard (PCI DSS). E-commerce merchants should ensure that data security language is present in all contracts with entities that store, process and/or transmit cardholder data on their behalf. These contracts should clearly identify roles and responsibilities for how cardholder data should be protected.

MasterCard recommends the following in their publication[2]:

- Merchants should employ strong security controls that follow industry best practices on their web-based environment, even if the environment is not in scope of PCI DSS requirements. Specifically: Secure Application Development, Regular Vulnerability Scans and Penetration Testing, Robust Patching, Intrusion Detection, Monitoring, and Network Security Controls (such as Firewalls). If a merchant's web environment has strong security controls in place, the risk of an attacker successfully compromising the environment can be greatly limited.
- While a merchant may be able to reduce or remove the scope of its environment's applicability to comply with PCI DSS requirements by using a hosted payments page, it does not remove the merchant's risk of being involved in, or even the source of, an account data compromise event. Merchants still have a duty to employ security controls based on industry best practices to their web-based environment to protect payment card data.

[1] http://visaeurope.com/en/businesses__retailers/payment_security/downloads__resources.aspx
[2] http://mastercard.com/us/company/en/docs/Hosted_Payment_Pages.pdf

PCI DSS Compliance Scope Impact Overview

The PCI Security Standards Council has developed the PCI DSS to mitigate the risk of compromise to a specific data set, i.e. payment card data. The standard is focused on the system components that are "within scope" of PCI. For all in-scope system components, all PCI DSS controls apply. The PCI DSS is based on industry security best practices but is not focused on the overall information security of merchants. To reduce PCI DSS compliance scope you must reduce the potential security risk and access to payment card data specifically.

The PCI Security Standards Council has incorporated scope reduction guidance within the PCI DSS framework, through FAQ guidance on specific technologies or architectures and published Emerging Technology Initial Roadmap documents. Compliance scope reduction has most commonly been addressed through the implementation of network segmentation where systems and environments that process, store or transmit sensitive authentication or cardholder data are "isolated" from other non-payment systems. This approach is not focused on reducing the applicability of any specific PCI DSS control to a merchant's environment but rather reducing the scope of the environment to which PCI DSS controls apply.

As most of the PCI DSS controls are designed to manage risk to cardholder data from specific threat scenarios, it is therefore possible to reduce their applicability by securing the card data in the merchant environment, so that the threat scenarios are no longer a viable risk. PCI DSS compliance scope reduction does not remove a merchant from the requirement to be PCI compliant. PCI DSS scope reduction does not eliminate a merchant's responsibility to validate compliance to their Acquirer. PCI DSS compliance scope reduction is only focused on addressing the applicability of specific controls to a merchant's environment based on "isolation" of data, systems and networks from security risks to payment card data.

PCI DSS compliance scope reduction's biggest payoff for merchants is the opportunity to eliminate the cost of PCI DSS control deployment for the sole purpose of meeting compliance obligations. The second major benefit is the reduction of cost and effort to validate PCI compliance of the merchant environment. Many merchants have sensitive data assets, other than payment card data, in their environment that have a risk of compromise. Reducing PCI DSS compliance scope for payment card data does not mean the PCI DSS controls are not justified to protect the merchants' other information assets.

HPE SecureData Web with HPE PIE Technology Impact on PCI DSS Scope

By encrypting cardholder data in the consumer's browser at the moment it is submitted for processing, by ensuring the security of the web infrastructure to protect unauthorized access to the e-Commerce hosting environment, and by developing a secure e-Commerce application to reduce the risk of vulnerabilities and protect the consumer-entered cardholder data, a properly deployed HPE SecureData Web with HPE PIE Technology solution can effectively "isolate" the majority of the merchant's environment from scope. If security best practices and system hardening guidelines are adhered to, the merchant network outside of the protected e-Commerce environment can be treated as an untrusted network and out of scope of PCI DSS when using strong data field and network transmission encryption.

Additionally, since a HPE PIE-integrated e-Commerce solution represents an attack surface and threat environment very similar to currently deployed hosted payments pages, acquiring banks and QSAs may make a risk-based determination to completely remove the merchant e-Commerce system from scope of PCI DSS, in the same way as hosted payments pages are generally treated today. This further reduces the overall cost of validating PCI DSS compliance for such a merchant.

However, implementing a HPE PIE technology-integrated e-Commerce solution or hosted payments page should not lower a merchant's level of sensitivity to the security of their e-Commerce environment and other sensitive assets. Merchants have the responsibility to implement security best practices for their web server and network infrastructure regardless of PCI DSS scope reduction.

Security Best Practices and System Hardening

As outlined above and further described by both Visa and MasterCard in their publications related to hosted payments pages, all merchants should prioritize the implementation of security best practices and system hardening in their internet-exposed environments to ensure an on-going high level of security. The PCI DSS standard was developed based upon a broad set of security best practices as applied to the protection of sensitive cardholder data. As a result, the following PCI DSS controls represent a good starting point, which merchants should use to establish a well-secured e-Commerce environment:

1. Perimeter Network Controls—Implement perimeter firewall(s) with locked down rulesets, IDS/IPS for on-going intrusion monitoring/prevention, etc. (see PCI DSS 1)
2. Logical Access Controls—Implement well-defined logical access controls for both local and remote users to ensure appropriate role-based access to devices in the merchant e-Commerce environment. (see PCI DSS 2, 8)
3. Host Configuration Controls—Implement patch and configuration management and anti-virus software to ensure on-going security of hosts in the merchant e-Commerce environment. (see PCI DSS 4, 5)
4. Application Security Controls—E-Commerce merchants who develop their own e-Commerce applications and independent application vendors should implement secure application development and on-going vulnerability assessment processes and mitigation strategies to ensure the security of their HPE PIE-integrated applications. Additionally, HPE SecureData Web service providers who implement a Host Decryption System using the HPE SecureData Host SDK, should implement secure application development and application hardening procedures for this crucial component of the full HPE PIE with HPE SecureData Web system. (see PCI DSS 6)
5. Implement system monitoring, file integrity management and activity logging on critical systems. (PCI DSS 10)
6. Create and deliver training to ensure personnel are aware of security policies and training (PCI DSS 11, 12)
7. Review the guidance provided by Visa and MasterCard in their publications related to hosted payments pages
8. Use publicly and freely available system hardening and configuration benchmarks/tools to ensure the on-going security of the merchant e-Commerce environment (cf. https://benchmarks.cisecurity.org/en-us/?route=default)

Security Review Summary of Findings

- HPE SecureData Web with HPE PIE Technology provides a unique solution to address the protection of consumer cardholder data entered via browser-based e-Commerce applications.
- HPE SecureData Web with HPE PIE Technology-integrated e-Commerce solution:
  - Implements National Institute of Standards and Technology's (NIST) AES FFX Format-Preserving Encryption (FPE) mode standard which offers HPE Format-Preserving Encryption (FPE) algorithm based on 128-bit AES encryption which offers stakeholders confidence that the cardholder data is indeed protected with strong encryption.
  - Allows an e-Commerce merchant to seamlessly integrate browser-context encryption of cardholder data into their existing e-Commerce application.
  - Reduces the risk of sensitive data compromise and removes exposure of plain text cardholder data to the e-Commerce merchant by encrypting the cardholder data in the consumer's browser and transmitting the encrypted data through the merchant network.
  - Represents an attack surface and threat environment similar to that of hosted payments pages.
  - Can significantly reduce PCI DSS scope and validation requirements similar to merchants implementing a hosted payments page solution.
  - Is aligned with the Visa Best Practices for Data Field Encryption published in October 2009.
- The merchant network outside of the protected e-Commerce environment hosting the HPE PIE technology-integrated e-Commerce application can be treated as an untrusted network and out of scope of PCI DSS as these systems no longer handle in-scope PCI data.
- Acquiring banks and QSAs may make a risk-based determination to completely remove the merchant e-Commerce system from scope of PCI DSS, thereby further reducing the cost of validating PCI DSS compliance.
- Implementing a HPE PIE technology-integrated e-Commerce solution or hosted payments page should not lower a merchant's level of sensitivity to the security of their e-Commerce environment. Merchants have the responsibility to implement security best practices for their web server and network regardless of PCI scope reduction.

Learn more at

voltage.com
hpe.com/software/datasecurity

4AA6-0204ENW, April 2016, Rev. 1