PCI Compliance and Scope Reduction

Achieve Rapid Compliance, Reduce PCI DSS Audit Scope and Cost, Neutralize Breaches End-to-end

The PCI DSS Backdrop to Data Privacy and Security

The Payment Card Industry (PCI) Data Security Standard (DSS) guidelines indicate that organizations processing and storing credit card data must comply with a set of well-defined audit requirements in twelve areas of cardholder data management and privacy. However, what is becoming increasingly clear is:

- Achieving and maintaining compliance with PCI DSS guidelines is expensive, challenging, time-consuming and disruptive as cardholder data is often stored, transmitted and used in many different applications within an organization, and often even beyond the IT perimeter.
- Compliance does not equal security, and compliance by itself is not enough to prevent data breaches. Cyber threats are increasingly sophisticated and hackers are going after data they can monetize, wherever they find vulnerability.
- Emerging new business initiatives—mobile, e-commerce, Cloud and Big Data projects bring more systems and applications into PCI scope as well as more risk.

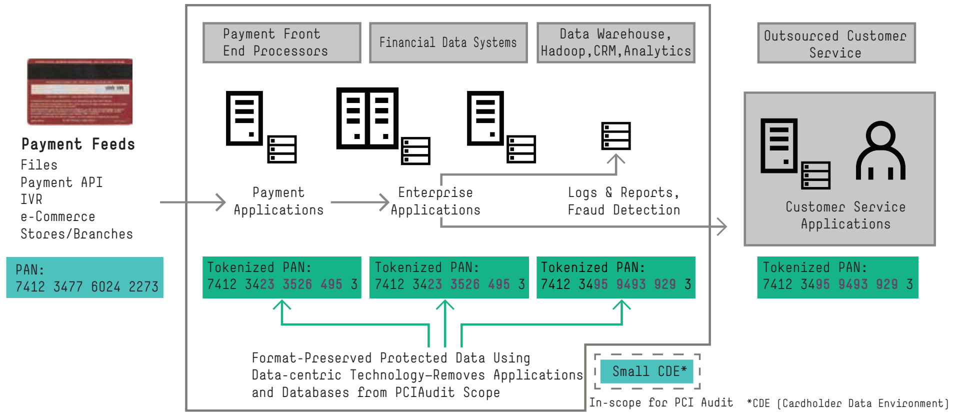
Tokenization, which is used as a way of replacing sensitive data like credit card numbers with tokens, is one of the data protection and audit scope reduction methods recommended by the PCI DSS. But, organizations who have adopted tokenization—either home-grown or first generation commercial solutions—have found it increasingly difficult to maintain compliance and are faced with growing complexity and rising costs resulting from conventional database-centric architectures. Others may have a hosted tokenization solution but would like to have more in-house control and a choice of processors.

Two Breakthrough Technologies for End-to-end Secure Commerce

HPE SecureData radically cuts compliance complexity and costs on an ongoing basis, and neutralizes data breaches by protecting sensitive data at the data field and sub-field level, in transit, in use and at rest. HPE SecureData provides a comprehensive data centric approach to PCI compliance that has been proven to reduce PCI DSS scope by up to 80%, cut compliance costs by up to 95%, and includes:

- **HPE Secure Stateless Tokenization (SST)** is an advanced, patent-pending, proven data security technology—stateless because it eliminates the token database that is central to other tokenization solutions and removes the need to store cardholder data. Eliminating the token database significantly improves the speed, scalability, security and manageability of the tokenization process. Every application handling the tokenized data, including back-end applications such as fraud analysis and loyalty programs, may be removed from PCI audit scope.
- **HPE SecureData Web with HPE Page-Integrated Encryption (PIE)** encrypts payment and personal data in browser-based transactions from the moment data is entered into a web browser and all the way through the web tier, the application tier, cloud infrastructure, and upstream IT systems and networks to the trusted host destination. This shields sensitive customer data from theft in front-end and intermediate systems, and further reduces audit scope.

Securing Enterprise Card Data Flows


Payment Front End Processors
Financial Data Systems
Data Warehouse, Hadoop,CRM,Analytics
Outsourced Customer Service
Payment Feeds
Files
Payment API
IVR
e-Commerce
Stores/Branches
Payment Applications
Enterprise Applications
Logs & Reports, Fraud Detection
Customer Service Applications
PAN: 7412 3477 6024 2273
Tokenized PAN: 7412 3423 3526 495 3
Tokenized PAN: 7412 3423 3526 495 3
Tokenized PAN: 7412 3495 9493 929 3
Tokenized PAN: 7412 3495 9493 929 3
Format-Preserved Protected Data Using Data-centric Technology–Removes Applications and Databases from PCIAudit Scope
Small CDE*
In-scope for PCI Audit
*CDE (Cardholder Data Environment)

SOLUTION CONSIDERATIONS	HPE SECUREDATA SOLUTION FOR PCI COMPLIANCE
How do I reduce PCI scope through tokenization of credit card numbers? Do I have to implement a token database to support the solution?	Up to 80% PCI scope reduction and 95% reduction in PCI compliance costs—Using format-preserved protected data removes applications from PCI scope, and enables applications to work without live data. HPE SST increases security by removing the need to store credit card data.
Does the solution encrypt data from my different payment channels (mobile, e-commerce, mobile onboard payments, call center) to eliminate gaps in data protection?	End-to-end Data-centric Protection—HPE SecureData Web secures payment and personal identity information (PII) in browser-based transactions by encrypting at the moment of capture and protecting it all the way through upstream IT systems and networks to the trusted host destination.
Can I use the same solution for my payment channels to reduce scope in my back-office systems? Will I have to rewrite these applications?	Easily brings applications out of scope without re-writes—HPE SST enables applications and databases to be fully protected and PCI-compliant without re-writing core business applications.
Is the solution standards-based, secure, and third party validated?	Proven Security Leadership track record—the HPE SecureData proven data protection technologies are standards-based (NIST, ANSI, IEEE, IETF), published, and third party validated.
How does this work with core payment transaction processing systems like mainframe and HPE NonStop?	Native tokenization—HPE SST delivers fully native tokenization on the IBM z/OS and the HPE NonStop OS for payment processor-grade performance and scalability.

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise

© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.