Hewlett Packard Enterprise

Business white paper

HPE SecureData Payments Solution—Processor Edition

For retail and e-commerce card processing environments

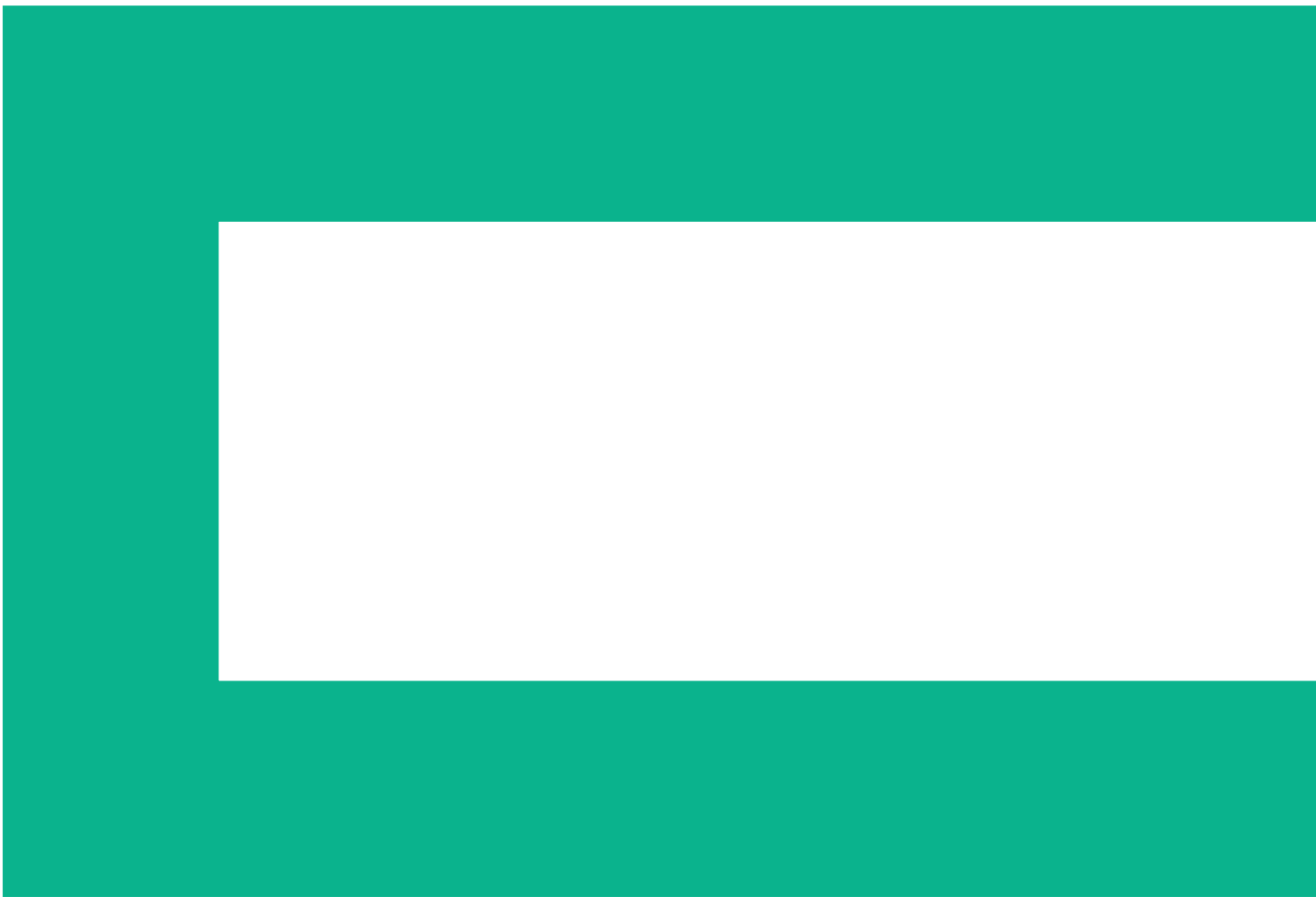


Table of contents

Introduction

This white paper describes HPE SecureData Payments Solution—Processor Edition which includes point-to-point encryption (P2PE) and patent-pending HPE Secure Stateless Tokenization (SST) for both card-present (CP) and card-not-present (CNP) processing environments.

HPE SecureData Payments Solution—Processor Edition is a complete security solution for protecting cardholder data from the moment of capture at the consumer endpoint until it reaches the payment processor. By providing persistent data-level protection, HPE SecureData Payments Solution—Processor Edition enables protection not only for authorization and settlement data flows but also for back office applications and processes that touch cardholder data. Through the use of unique HPE Security—Data Security technologies, HPE SecureData Payments Solution—Processor Edition eliminates the traditional complexities associated with key injection, key management, and deployment, while reducing PCI DSS scope dramatically.

HPE Security—Data Security Technology Leadership

HPE Security—Data Security simplifies data protection with innovations such as: HPE Identity-Based Encryption (IBE), for key management without public key infrastructure (PKI) and HPE Format-Preserving Encryption (FPE), a technique which renders data useless to attackers yet still useful to business processes; HPE Page-Integrated Encryption (PIE) for securing browser-based transactions; and patent-pending HPE Secure Stateless Tokenization (SST) for protecting data at rest.

HPE Security—Data Security protects data in transactions, fields, files, applications, databases, and back office workflows from legacy applications to cutting-edge cloud systems.

Among HPE Security—Data Security customers are six of the top eight U.S. payment processors including Heartland Payment Systems and Vantiv, thousands of retailers, and a top payment gateway in both Europe and the U.S. HPE SecureData Payments partners include leading device manufacturers such as Ingenico and Equinox.

The Payment Security Challenge

In the last few years there have been dramatic changes in the payment ecosystem. Many of the changes relate to security—or the lack of security—throughout the payment ecosystem. Exploitation of security vulnerabilities resulted in well-publicized data breaches that damaged consumer confidence and ensured regulatory compliance with Payment Card Industry Data Security Standard (PCI DSS) remains an expensive and time consuming activity.

The impact of payment ecosystem changes and the resulting regulations have reduced business agility for acquirers, payment gateways, merchants and others. It is essential to protect cardholder data against threats by using technologies, such as point-to-point encryption for protecting cardholder data from capture all the way through to the processor and tokenization for protecting post authorization cardholder data.

Today's challenges can be characterized as:

- Defending from data breaches by criminal attackers: Sophisticated attacks to obtain cardholder data by well-funded criminal hacking groups are increasingly common. Since stolen data can quickly be transformed into cash, breaches will increase in scale and velocity if unchallenged. The industry's attempts to prevent such attacks from a traditional IT security perspective have failed as evidenced by the number of breaches that happen every day.
- Reduction or elimination of costs to comply with PCI DSS: There is an overwhelming desire to reduce costs and complexity involved in achieving and validating compliance with PCI DSS. At the same time, it must be understood that PCI compliance does not mean data security. Investments must be made to reduce security risk as well as compliance costs.

- Lower operating margins: Spending on PCI DSS compliance is a barrier to business growth as funds being spent on compliance and validation are unavailable for investment in core competencies and innovation.
- A desire to extend existing infrastructure for maximum lifespan: Existing IT platforms are reaching their acceptable risk thresholds in light of new persistent threats. Given the reality of today's economic pressures, the ability to extend infrastructure lifespan without sacrificing security is needed.
- The rise of new payment and customer service channels: Consumers can no longer be forced to transact with a merchant through a single channel. Merchants must secure m-commerce, e-commerce and retail POS endpoints to compete in today's marketplace and to do so effectively and efficiently.

Unique HPE Security—Data Security Technology

HPE SecureData Payments Solution—Processor Edition is built on breakthrough cryptographic technologies: HPE Format-Preserving Encryption (FPE) and HPE Identity-Based Encryption (IBE). HPE FPE and HPE IBE combine with HPE Secure Stateless Tokenization (SST) and HPE Page-Integrated Encryption (PIE) to create a unique security solution that addresses the challenges associated with the payment ecosystem which traditional security approaches cannot address.

HPE Format-Preserving Encryption

HPE Format-Preserving Encryption (FPE) is a symmetric key technology based on AES that allows for structured data to be strongly encrypted while maintaining its original format. For example, a 16-digit credit card number can be encrypted such that the resulting output is also 16 digits. In addition, internal properties of the data such as checksums can be maintained; the encrypted 16-digit value can be guaranteed to have a valid Luhn checksum (or, if desired, an invalid checksum). Unlike other approaches, HPE FPE is not limited in the data sizes that can be encrypted. For example, other implementations may require a full Primary Account Number (PAN), or often times a full track, in order to encrypt. HPE FPE can handle any data size, from a subset of digits up to long strings of text. This allows for sub-elements of the PAN, such as the middle 6 digits, to be encrypted in isolation, while maintaining the rest of the PAN or track in the clear, without sacrificing encryption strength.

Additionally, HPE FPE is not restricted to use for encrypting numeric values; it can be applied to structured data of any type, including alphanumeric fields, decimal values, and dates. HPE FPE is backed by a strong security proof that validates it has the same security as the underlying block cipher, AES.

HPE Identity-Based Encryption

HPE IBE is a public-key algorithm that eliminates the primary complexity associated with traditional PKI systems: digital certificates. Like existing public-key systems such as RSA, HPE IBE employs separate encryption (public) and decryption (private) keys. HPE IBE, however, allows an arbitrary string to be used directly as a public key, while the private key is generated mathematically by a key server.

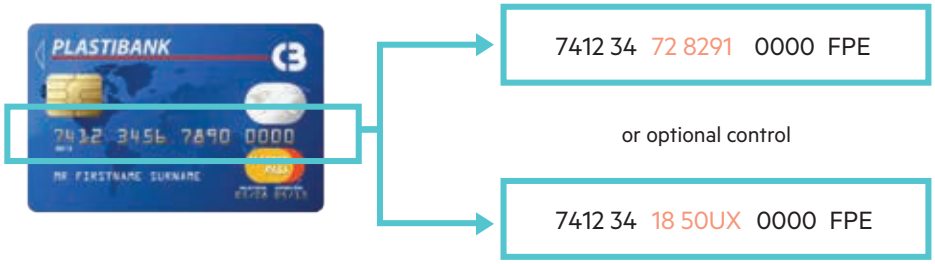


Figure 1: HPE Format-Preserving Encryption illustration showing the format of the credit card being preserved in two examples.

Thus, rather than needing to use a digital certificate to associate a public key with a recipient (e.g., 'recipient@domain.com'), HPE IBE allows that recipient's identifier to be used directly for encryption. This capability eliminates the need for certificate generation, issuance, distribution, and revocation, resulting in a key management architecture that is far easier to deploy and manage. HPE SecureData Payments Solution—Processor Edition extends the use of HPE IBE to enable powerful yet flexible key management architecture for point-to-point encryption at processor grade scale.

HPE SecureData Payment Solution Encryption Key Management

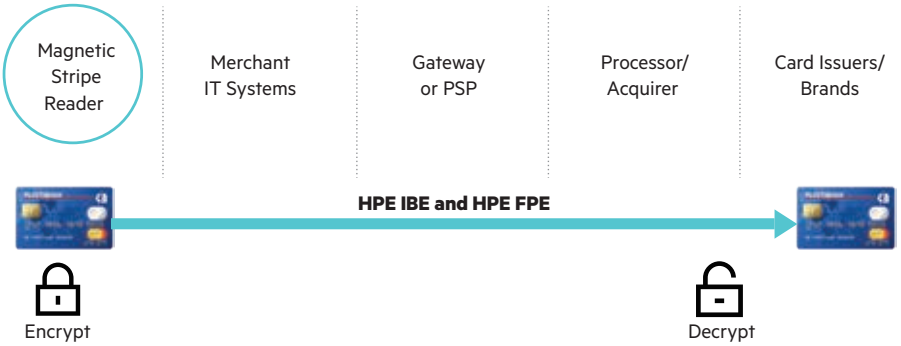


Figure 2: The use of HPE FPE and HPE IBE technology combined in enabling point-to-point protection of data from capture to hand off.

Unlike traditional key management architectures which are highly stateful and require continuous backup, replication, and management of randomly-generated keys, HPE SecureData Key Management is completely stateless. Keys are generated on-demand using a Key Derivation Function (KDF), reducing the need to cache or store keys on the server. This design enables a secure architecture that is dramatically more scalable and requires far less maintenance than legacy systems.

Identity-Based Key Encapsulation and Encryption Protocol (IBKEEP)—An Injectionless Encryption Protocol

The combination of HPE FPE and HPE IBE creates a convenient protocol which can permit point-to-point encryption of cardholder data while minimizing key management overhead. This protocol is referred to as IB-KEEP. IB-KEEP eliminates the pain of key injection by minimizing changes to existing infrastructure and code bases.

There is a diverse set of transaction initiation points that capture and transmit cardholder data. The IB-KEEP protocol aims to protect cardholder data in existing environments, acknowledging that systems without dedicated security hardware are inherently vulnerable to attacks. We classify these systems into three groups:

- **Hardware with tamper-resistant security module (TRSM)/Secure Cryptographic Device (SCD).** These are POS devices (typically terminals) capable of running security code in a mode where the payment application on the device is incapable of altering the operation of the security code, or reading the memory of the security code. On these devices, PAN data passes directly from the reading device (mag stripe reader or keypad) to the security code.
- **Hardware without tamper-resistant security module (TRSM)/Secure Cryptographic Device (SCD).** These are devices, often running in a fixed-function manner, that do not have full isolation between the application code that generates payment messages and the hardware running the security code.
- **Software.** These are devices (typically PCs) running POS applications that accept PAN data input from a stock keyboard or from an unsecured magnetic stripe reader.

HPE SecureData Payments Solution—Processor Edition

Implementation

HPE SecureData Payments Solution—Processor Edition is a suite of products and provides all of the necessary components to protect cardholder data at consumer capture all the way through to processing host. The products are:

- HPE SecureData Payments
- HPE SecureData Web
- HPE SecureData Enterprise with HPE Secure Stateless Tokenization

The kit includes: SDKs to encrypt CP and CNP cardholder data at capture, and back-end host-side decryption tools and HPE SST technology.

HPE SecureData Terminal SDK for retail and e-commerce

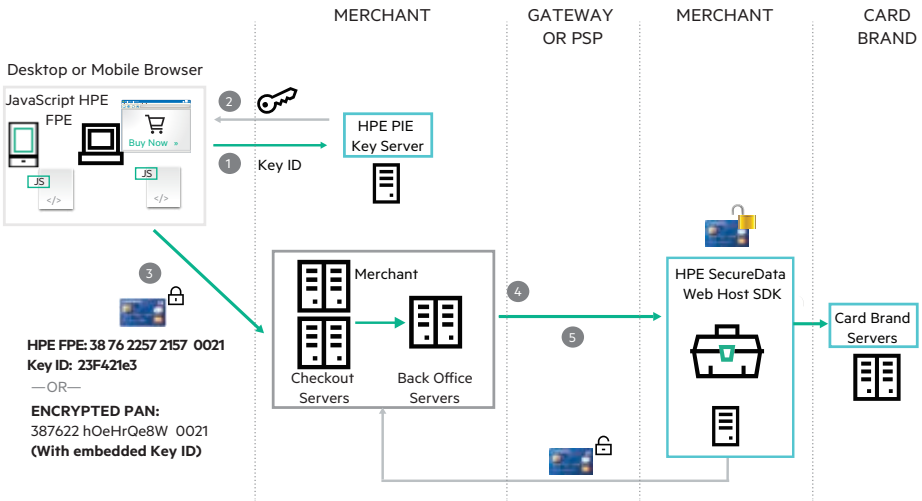
The HPE SecureData Terminal SDK is highly portable and is designed to operate with minimal hardware requirements.

On a physical POS terminal, the HPE SecureData Terminal SDK may be implemented either at the operating system or firmware layer or within the software application. Implementing within the operating system can allow for sensitive data to be hidden from the software application thus reducing PCI scope. However, in cases where implementation in the operating system is difficult or infeasible, the HPE SecureData Terminal SDK can be integrated into the application without compromising security: because keys are never stored (and can be rotated on-demand), TRSM or SCD-based symmetric key storage is not required. The HPE SecureData Terminal SDK approach of using HPE FPE and HPE IBE together to eliminate static key injection and storage issues are preferred. However, the HPE SecureData Terminal SDK can also adopt alternative key management approaches with software adjustment and corresponding key management processes for key injection. This flexibility permits the HPE SecureData Terminal SDK to be adapted to any scenario, and capabilities can be combined to permit migration to lower cost approaches in timescales suited to merchant hardware refresh cycles.

HPE Page-Integrated Encryption technology for card-not-present processing

HPE PIE technology in HPE SecureData Web handles encryption in e-commerce environments, including virtual terminals and shopping cart software. HPE PIE builds upon HPE FPE and HPE Stateless Key Management to encrypt cardholder data entered into browsers on any device from capture all the way through to decryption for processing. Cardholder data remains encrypted as it moves through the merchant's environment such that plain text data is not exposed to the merchant.

Merchants retain full control over their consumer checkout process and avoid third-party hand-offs which can result in consumer abandonment of the checkout process.



1. JavaScript HPE FPE package, Key, ID provisioned on page load over HTTPS
2. Invoked by web application via 1 line of code
3. Single use Encryption of CC#—unique per transaction
4. Merchant cannot decrypt and has no key access
5. Only the processor can recover key to recover the PAN using Host SDK

Figure 3: HPE SecureData e-commerce protection

HPE SecureData Host SDK

On the back-end, HPE Security—Data Security provides a rich set of integration capabilities to enable decrypting of data encrypted with the HPE SecureData Terminal SDK and HPE SecureData Web.

The HPE SecureData Host SDK provides an integration toolkit as pre-built libraries available on z/OS, Stratus VOS, HPE NonStop and various UNIX, Windows and Linux platforms. This API permits decryption of incoming cardholder data, resolves incoming keys for decryption of data and can re-encrypt PAN data for local storage in a normalized fashion. Decryption and re-encryption operations take place inside the physical confines of an HSM.

HPE Secure Stateless Tokenization Technology

HPE Secure Stateless Tokenization offers fully integrated tokenization capability to protect cardholder data that must be stored for back-office operations and follow-on transactions. HPE SecureData Enterprise with HPE Secure Stateless Tokenization (SST) does not index tokens on a database; rather token tables are pre-generated and operate in system memory. The pre-generated token table can reside in multiple data centers to ensure that the same token is returned for any given PAN regardless of which data center processes the transaction. Since tokens are created in memory and no read-write operations occur, HPE SST offers a significant performance advantage over traditional tokenization deployments.

HPE SST solves the token collision problem that can occur with traditional tokenization deployments in high-availability processing environments with more than one data center.

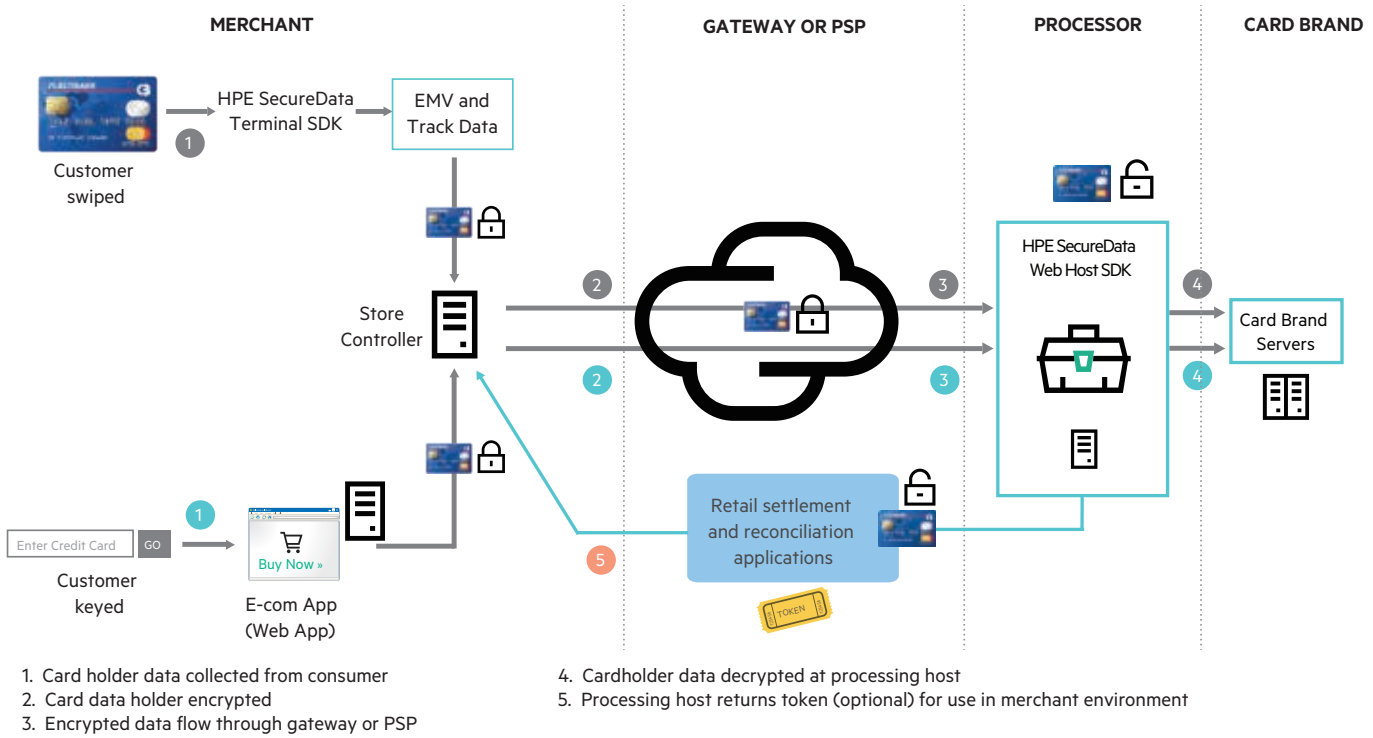


Figure 4: Generalized payment flow with cardholder data encryption and tokenization

Benefits of HPE SecureData Payments Solution—Processor Edition

COMPONENT	PROTECTS	SCOPE REDUCTION
HPE SecureData Terminal SDK for card- present processing	CHD in motion (transmitted, processed)	Up to 79% scope reduction for merchants using dial-up connections Up to 69% scope reduction for merchants using an IP connection
HPE SecureData Web—HPE Page-Integrated Encryption technology for card-not-present processing	CHD in motion (transmitted, processed)	Up to 100% scope reduction Can completely remove the merchant's CNP system from scope
HPE SecureData Enterprise—HPE Secure Stateless Tokenization technology	CHD at rest (stored)	Up to 100% scope reduction in terms of PCI DSS requirements 3 and 9

HPE SecureData Payments Solution—Processor Edition has been independently validated to reduce scope and costs of compliance of up to 79% in CNP environments, and up to 100% PCI scope reduction can be achieved, as assessed independently by Coalfire, an industry leading QSA.

Reduction in Operational Costs and Complexity

- No Key Injection: Through the use of HPE IBE, HPE SecureData Payments Solution- Processor Edition eliminates the need for key injection. Encryption keys are dynamically generated by the terminal and can be rotated on demand.
- Stateless Operation: Unlike other architectures, HPE SST key management is completely stateless: encryption keys never need to be stored, replicated, or backed up. This enables a key management system that is far easier to deploy and far easier to maintain and manage.

Robust Host-Side Capabilities

- Broad Platform Support: HPE SecureData offers native encryption and decryption capabilities on a wide variety of platforms, including Windows, Linux, UNIX, and z/OS. This breadth of coverage provides for the highest performance, as decryption of data can take place on existing systems, without introducing network latencies and for maximum flexibility to adapt to complex use cases and risk requirements.
- Multiple Integration Options: By providing multiple integration choices, including SDKs, HSM options, web services, and command line tools, HPE SecureData Payments Solution- Processor Edition enables encryption to be incorporated into a wide variety of systems. Thus, protection can be extended beyond authorization and settlement to all applications interfacing with PCI data.
- Multiple Data Protection Options: With built-in encryption using standard AES, format-preserving AES (FFX mode AES), HPE IBE and bulk encryption, randomly generated tokens and token vaults, file encryption for whole files, field level encryption, or COBOL Copybook format data encryption, HPE SecureData Payments Solutions—Processor Edition provides a complete range of protection options under one system—maximizing ROI and use case, with the flexibility to switch between methods by policy.

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

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0218ENN, April 2016, Rev. 1