Hewlett Packard Enterprise

Point-to-point payment data protection

Verifone payment devices support HPE SecureData Payments encryption for secure transactions

Business benefits

- Industry standards-based data-centric security
- Complete solution for PCI scope reduction
- Multiple integration options
- Eliminates Operational Key Complexities
- End-to-end data protection

The payments challenge: Criminals are targeting credit cards

Cardholder data is a high-value target for criminals, as seen in the frequency and size of recent credit card breaches. When data is exposed, it puts customers and businesses at risk of financial loss. The industry's EMV chip card initiative focuses on card authentication, but does not reduce the likelihood of cardholder data breaches. However, when EMV chip technology is combined with PCI Security best practices, businesses significantly strengthen their ability to mitigate data breach risks while protecting credit card data at rest and in transit within their environment. HPE SecureData Payments provides a perfect complement to EMV with point-to-point encryption and tokenization solutions for retail payment transactions by removing data loss vulnerabilities, and significantly reducing PCI audit scope for businesses.

The solution: Embrace the data-centric approach to security

HPE SecureData Payments protects payment data at all points, from swipe through to the payment processor, end-to-end. It eliminates the traditional complexities associated with payment device key injection, key management, payment application changes, and enables a true end-to-end architecture that can be rapidly deployed even in the most complex environments. By protecting the data itself, HPE SecureData Payments eliminates security gaps that exist between networks, databases, and applications, which is typically where malware targets. Enabling HPE SecureData Payments can reduce the cost of complying with the PCI DSS—a direct result of reducing the number of changes necessary to implement payment security and eliminating sensitive PCI data from the payment ecosystem.

HPE SecureData Payments provides a complete payment transaction protection framework, built on two breakthrough technologies encompassing encryption and key management: HPE Format-Preserving Encryption (FPE) and HPE Identity-Based Encryption (IBE). These two technologies provide a unique architecture that addresses the complexity of retail environments with high transaction volume.

Benefits/value proposition

Industry standards-based data-centric security: HPE FPE is a NIST-approved standard supported in Verifone's contemporary line of devices—Verifone VX devices using SoftPay, MX terminal payment devices, and E-Series mobile hardware devices.

PCI scope reduction: End-to-end encryption can easily be combined with HPE SecureData Web and HPE Secure Stateless Tokenization to provide merchants with complete protection of PCI data from all acceptance points and throughout its lifecycle in your data environments.

Multiple integration options: HPE SecureData Payments is pre-loaded into many payment devices and ships with millions of payment devices globally. To facilitate decryption and tokenization, processors, and merchants may implement the HPE SecureData Payments infrastructure in numerous host-processing environments.

Eliminates operational key complexities: Unlike legacy key management solutions, HPE SecureData Payments support all encryption/decryption and tokenization/detokenization functions through the management of only one host-side key.

End-to-end data protection: Businesses may activate HPE SecureData Payment's point-to-point encryption and tokenization solutions with many leading payment transaction acquirers and gateways, or within their own data center environments. As a result, sensitive PCI data never touches insecure areas of your payments ecosystem.

Stand-alone
Verifone VX805, 520, 820, 680, 690

Integrated
Verifone MX 915, 925

Mobile peripheral
Verifone E315, 335, 355

HPE Format-Preserving Encryption

With HPE Format-Preserving Encryption (FPE), HPE SecureData Payments removes all sensitive data by encrypting PCI data in a format that is preserved so that it doesn't disrupt the payment authorization process. This eliminates the need to modify intermediary payment systems to accommodate an unknown data format. Data properties are maintained, such as a checksum, and portions of the data can remain in the clear. This aids in preserving existing business processes such as BIN routing or use of the last four digits of the card in customer service scenarios.

HPE Stateless Key Management

HPE SecureData Payments is based on HPE Identity-Based Encryption (IBE)—a breakthrough in key management that eliminates the complexity of traditional Public Key Infrastructure (PKI) systems and symmetric key systems. With traditional symmetric encryption, encryption keys must be injected at startup and rotated regularly, which is operationally and logistically challenging. With HPE SecureData Payments, encryption keys are securely generated on demand within the payment device, which eliminates encryption key management requirements.

Supported Verifone devices

HPE SecureData Payments encryption can be activated on Verifone VX, MX, and E-Series devices to protect PCI data. Through a simple firmware upgrade, businesses can turn on encryption so that sensitive data remains fully protected and format-preserved in transit to a designated decryption point. Now, businesses have an expanded number of payment device options, on which they can use HPE SecureData Payments.

Complimentary HPE SecureData Payments security solutions: HPE Secure Stateless Tokenization and HPE SecureData Web

Point-to-point encryption can easily be combined with HPE SST to provide merchants with a complete solution for reducing PCI audit scope. HPE SST replaces PAN data after authorization with randomly generated tokens, which reduces the risk of data theft and removes merchant systems from PCI scope without the cost and complexity of maintaining a token vault database.

HPE SecureData Web protects payment data captured at the browser, from the point the customer enters their cardholder information or personal data, and keeps it protected through the Web, the application, cloud infrastructure, and upstream IT systems and networks to the trusted host destination.

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

Sign up for updates

Hewlett Packard Enterprise

4AA6-5577ENN, June 2016