Voltage security

DATA SHEET
Voltage SecureData Payments

End-to-end Protection for Payment Data

DRAMATICALLY LOWER MANAGEMENT AND COMPLIANCE COSTS

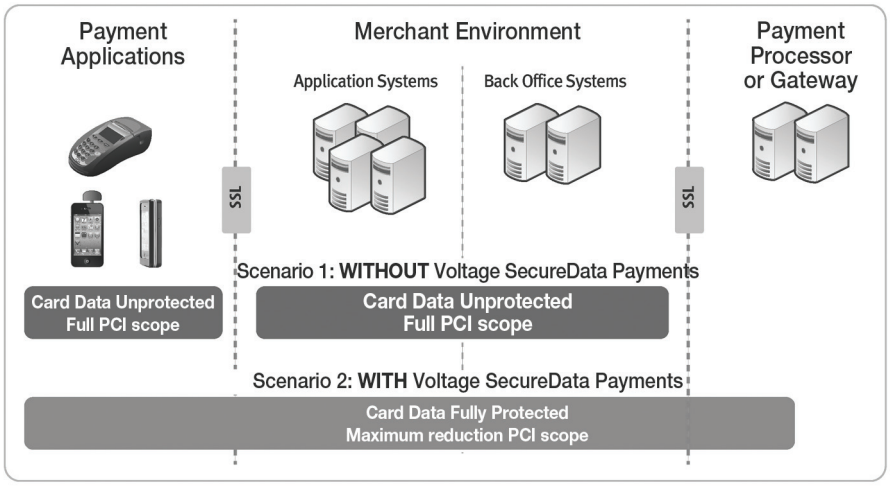
The Challenge – Payment Data Streams Must be Protected End-to-end

In today's environment of heightened regulatory requirements and increasing risk of cardholder data breach, it is critical for merchants, payment processors, and acquirers to protect payment data anywhere it moves, anywhere it resides, and however it is used.

In payment acceptance systems payment data is commonly left unprotected during the authorization and settlement processes. Payment data is also left unprotected during routine and necessary back-office business processes such as fraud screening, chargeback processing and recurring payment processing. Common methods for protecting payment data are often inflexible, expensive, and difficult to implement.

Voltage SecureData Payments Protects, Simplifies, Reduces

Voltage 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, Voltage SecureData Payments eliminates security gaps that exist between networks, databases and applications when protected with point security solutions are used.

Enabling Voltage 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 data protection and eliminating payment data from databases and applications.

Innovation in Cryptography Provides End-to-end Encryption without Massive Changes

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

Format-Preserving Encryption

With Voltage Format-Preserving Encryption (FPE), credit card numbers and other types of structured information are protected without the need to change the data format or structure. In addition, data properties are maintained, such as a checksum, and portions of the data can remain in the clear. This aids in preserving existing processes such as BIN routing or use of the last 4 digits of the card in customer service scenarios.

Identity-Based Encryption

Identity-Based-Encryption (IBE) is a breakthrough in key management that eliminates the complexity of traditional Public Key Infrastructure (PKI) systems and symmetric key systems. In other words, no digital certificates or keys are required to be injected or synchronized. IBE also enables end-to-end encryption from swipe-to-processor and swipe-to-trusted-merchant applications.

With POS solutions that use legacy symmetric encryption, encryption keys must be reset annually for each POS device through a process called key injection. This procedure is expensive and cumbersome, as merchants must take POS devices offline while new keys are injected. With Voltage SecureData Payments, because encryption keys are securely generated on demand and not stored, POS devices are not subject to key injection and key rotation. This function happens systematically, eliminating labor-intensive key management processes and costs.

Voltage SecureData Payments Compatibility

- **Robust Host Side Capabilities and Broad Platform Support:** Voltage SecureData Payments Host SDK can be deployed on a wide variety of platforms including HP NonStop, Windows, Linux, UNIX, z/OS and Stratus. Voltage SecureData is the only data protection solution available that natively runs on Stratus VOS, enabling maximum protection and efficiency.
- **Multiple Integration Options:** Processors and merchants can choose to integrate using SDKs, web services, and/or command line tools for quick and simple deployment. End-to-end encryption can easily be combined with **Voltage Secure Stateless Tokenization (SST)** to provide merchants with a complete solution for reducing PCI audit scope.
- Integrated POS Systems: Voltage SecureData Payments POS SDK integrates easily into a variety of POS devices and platforms. Voltage SecureData Payments can also support devices with Tamper Resistant Security Modules (TRSMs). For a complete list of payment partners, visit **voltage.com/partners**.
- **Light-weight Mobile Integration:** For mobile terminals or sleeves that accept payment data, Voltage offers a light-weight POS SDK that accommodates the low power and small memory requirements to support mobile form factors.

How Secure is Secure?

To ensure compliance with Visa and PCI DSS best practices and requirements, Cryptographic Assurance Services, LLC (CAS), a leader in cryptographic compliance consulting, has conducted an independent security review and verified that Format-Preserving Encryption conforms with the complete list of Visa's global industry best practices for data encryption, and the PCI DSS encryption requirements.

ABOUT VOLTAGE SECURITY

Voltage Security®, Inc. is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption and key management solutions, enabling our customers to effectively combat new and emerging security threats. Leveraging breakthrough encryption technologies, our powerful data protection solutions allow any company to seamlessly secure all types of sensitive corporate and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.

For more information, please visit **www.voltage.com**.

v04232013

Voltage Security, Inc. US Tel: +1 (408) 886-3200 EUR Tel: +44 (0) 203 468 0559 www.voltage.com/contact