Voltage SST Technology Delivers Advanced Protection for Sensitive Corporate Data

DRAMATICALLY REDUCES PCI DSS AUDIT SCOPE, CUTS COSTS AND COMPLEXITY

Introduction

Enterprises, merchants and payment processors face severe, ongoing challenges securing their networks and high value sensitive data such as payment cardholder data, to comply with the Payment Card Industry Data Security Standard (PCI DSS) and data privacy laws.

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. Enterprise users, merchants and processors, however, are facing new and mounting compliance costs and complexities as they discover that conventional, first-generation tokenization solutions aren't able to support business evolution and growth.

Voltage Secure Stateless Tokenization (SST) Technology

There is a new tokenization technology for companies that want to reduce compliance scope, cut costs and complexity, and maintain business processes with advanced security – not just on implementation, but also as the business evolves and grows.

The Voltage Security SST technology is an advanced, patent pending, data security solution that provides enterprises, merchants and payment processors with a new approach to help assure protection for payment card data. Voltage SST technology is offered as part of the Voltage SecureData Enterprise data security platform that unites market-leading Voltage Format-Preserving Encryption, Voltage SST technology, data masking and Voltage Stateless Key Management to protect sensitive corporate information in a single comprehensive solution.

Voltage SST technology is "stateless" because it eliminates the token database which is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. Voltage Security has developed an approach to tokenization that uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual "appliances" – commodity servers – and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with SST technology, thus improving the speed, scalability, security and manageability of the tokenization process.

Security Proof

Voltage SST technology is designed to substantially increase data security over alternative tokenization solutions. Eliminating token databases and stored data also removes high-value data targets for hackers, and reduces the risk of data breach. With Voltage SST technology, the resulting tokens cannot be related back to the original sensitive data.

Additionally, Voltage SST technology has been developed by cryptography experts, is based on published and proven academic research and standards, and validated by a top third-party Quality Security Assessor (QSA) and independent cryptography experts. It effectively mitigates risk of security breaches, and is proven for PCI DSS compliance and maximum audit scope reduction.

The Voltage SST Technology Difference

Reduced compliance scope and costs

Voltage SST removes the storage of card data, and does so without requiring token databases that are mapped to the underlying card data and are costly to maintain. This dramatically reduces the number of applications and systems that are considered in-scope for compliance assessments. Eliminating token databases from the solution:

- Eliminates the cost of external database hardware and software acquisition and/or licensing and replication software.
- Means no database growth over time, which is often a cause of performance degradation, and no replication and backup issues.

Increased protection and reduced security risk

Eliminating token databases and stored credit card numbers removes the high value sensitive data that could be targeted through an attack.

- Voltage SST technology delivers token lookup tables with random numbers that cannot be related back to sensitive data.
- The static tables are securely replicated to all servers where tokenization will occur.

Increased business performance and responsiveness

The SST architecture assures high availability and throughput to support any current business processes. For transaction processors, including payment switches, tokenization service providers, and card issuers, Voltage SST technology is a secure, high-performance solution that meets carrier-grade and payment-processor grade high availability requirements, provides 100% data consistency, and will scale linearly so that they can generate hundreds of millions of tokens to represent card numbers for internal use or to provide tokenization service to merchants.

Voltage SST is designed for high performance to support business processes and demand growth.

- High-speed tokenization is performed in-memory without bottle-necking or degradation.
- There are no software pre-requisites. Voltage SST works with virtually all languages and platforms, so the solution integrates easily into existing IT environments, including mainframe and mid-range.
- Scalability is linear, providing capacity for distributed enterprises and predictable capacity increases for high-growth businesses or seasonal demand peaks.

Benefits for Your Business

- Dramatically reduce compliance scope, cost and complexity
- Increase protection of sensitive data and reduce risks of breach
- Support the business with high performance, carrier-grade and payment-processor grade high availability, 100% data consistency, and linear scalability

> *Secure Stateless Tokenization represents a paradigm shift in tokenization. It provides service at higher performance and with greater security than conventional, database-centric solutions...*
>
> *- Coalfire*
> *a leading independent IT Governance, Risk and Compliance firm*

FEATURES	BENEFITS
No Pre-requisites	Works with all platforms and languages; easily integrates with existing IT environments.
Fast Deployment	Voltage SST can be deployed and configured in hours and integrated with applications in a few days.
Data Integrity	Added servers never introduce data integrity issues or a need for synchronization. 100% consistent, 1-to-1 mapping between PAN input and token is provided by all servers in all data centers. SST technology ensures that business applications using tokens (loyalty, marketing, fraud, etc.) work exactly as they did with PANs.
Optional Client-side Tools	Tokenization can be performed using local API calls or command-line operations, and can be scripted for high-throughput batch operations (e.g. z/OS mainframe applications) with very high performance and security, never leaving the application environment.

Features and Benefits continued on next page...

Rapid Key Rollover	Rotating the encryption key that protects the token lookup tables distributed across all servers is a single, efficient, high-speed process that takes just minutes to execute, even during live operations. There are no token keys to manually manage, replicate, or recover.
Dual Controls	Sensitive operations are protected by dual controls – as mandated by PCI DSS compliance guidance. Voltage dual controls are workflow-based, promoting efficiency as well as security.
Layered Authentication & Authorization	Authentication methods can be applied individually or layered for added security. Methods include: LDAP, Active Directory, digital certificates, IP address verification and custom credential stores; authorization can make use of existing groups in LDAP or Active directory to simplify configuration of fine-grained permissions.
Fine-grained Tokenization Permissions	Reduce the PCI DSS scope of certain applications while still allowing them to make use of partially de-tokenized PAN data. Enables control of scope by controlling exactly what applications are allowed to do: tokenize only, de-tokenize only, or partial de-tokenization with certain digits blocked.
Rich Formatting Options	The format of tokens can be configured to best preserve functionality in applications that previously used actual card numbers – eliminating costly application changes. Tokens can also be configured with substitute alpha characters to enable auditors to clearly distinguish tokenized data.
Token Multiplexing	PCI DSS guidance points to the need to make tokens meaningful and usable only to the particular group of applications that require them. Token Multiplexing provides a simple way to create token independence between merchants, applications, or lines of business, avoiding the cost and complexity of multiple database lookup tables. Token multiplexing can be used to remove high value tokens from scope.
Enterprise-wide Data Protection	Voltage SST technology is part of Voltage SecureData Enterprise, delivering market-leading encryption, tokenization, data masking and key management in a single unified architecture for enterprise-wide data protection.
Front-door PCI Scope Reduction	In addition to SST technology, Voltage SecureData also delivers technologies to substantially reduce PCI scope in use cases where tokenization doesn't fit: • Voltage SecureData Web takes e-commerce web servers up to 100% out of scope • Voltage SecureData Payments POS solutions support PCI compliance at physical card-swipe devices

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**.

v04142013