Voltage SST Technology Protects Sensitive Data and Dramatically Reduces PCI DSS Audit Scope

CUT COSTS AND COMPLEXITY; MAINTAIN BUSINESS PROCESS WITH ADVANCED SECURITY

Introduction

Merchants, service providers, and enterprises face severe, ongoing challenges securing payment card data. Tokenization – replacing card numbers with tokens – is one method of data protection and audit scope reduction recommended by the Payment Card Industry Data Security Standard (PCI DSS).

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 your business grows and evolves.

The Voltage Secure Stateless Tokenization™ (SST) 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 and sensitive corporate data. Voltage SST technology is offered as part of the Voltage SecureData™ enterprise data security platform that unites market-leading encryption, tokenization, data masking and key management to protect sensitive corporate information in a single comprehensive solution. Voltage SST technology is deployed and in use with customers leading in payment card processor, retail and airline industries.

The SST technology is "stateless" because it eliminates the token database and removes the storage of card data from the solution. This dramatically improves speed, scalability, security and manageability over conventional tokenization solutions.

PCI DSS Scope Reduction Analysis for SST by Coalfire

Voltage Security® engaged Coalfire Systems, Inc. (Coalfire) as a respected PCI Qualified Security Assessor (QSA) company to conduct an independent review of its SST technology. Specifically, Voltage wanted to accomplish the following:

- Confirm that the technology would support a customer's overall PCI compliance efforts, and
- Determine how it would reduce the audit scope of a merchant's cardholder data environment (CDE)

Coalfire performed an intensive technical review and documented the analysis.

Excerpts from the analysis are included as noted in this brief. The full report is available on request from Voltage Security: ask for "**PCI DSS Scope Reduction Analysis for Voltage Secure Stateless Tokenization**" by Coalfire.

In addition to excerpts from Coalfire's independent review, this document also contains brief descriptions of several Voltage SST implementations in customer environments.

Excerpt: *Coalfire Executive Summary*

"The SST methodology was designed with two types of customers in mind. First are merchants and enterprises that handle credit card numbers and that are looking to reduce scope by bringing tokenization in-house. This gives the merchant more flexibility since it is not bound to a particular processor for tokenization solutions. As with an outsourced solution, the merchant would benefit from reduced scope since cardholder data would not be stored in the environment (due to the unique way the SST method assigns tokens).

"The second type of customer includes transaction processors, payment switches, tokenization service providers, and card issuers. (These are referred to collectively in this report as 'processors'.) These customers are not primarily interested in scope reduction. First and foremost, they want a secure, high-performance solution that will scale linearly so that they can generate hundreds of millions of tokens to represent card numbers used at thousands of merchant locations. These tokens could be for internal use or to provide tokenization service to merchants.

"By employing SST technology, both classes of customers should realize scope reduction as shown in this table."

> *Voltage Secure Stateless Tokenization represents a paradigm shift in tokenization. It provides service at a higher performance and with greater security than conventional, database-centric solutions. It is Coalfire's opinion that Voltage Stateless Tokenization, when properly implemented, would effectively promote PCI compliance goals and reduce PCI audit scope for merchants and processors alike.*
>
> *- Coalfire*
> *PCI DSS Scope Reduction Analysis for Voltage Stateless Tokenization*

Summary of PCI DSS Scope Impact

● merchant ● processor

PCI DSS Requirement	Scope Reduction Impact		
	Major	Partial	Minor
1. Install and maintain a firewall configuration to protect cardholder data.			● ●
2. Do not use vendor-supplied defaults for system passwords and other security parameters.			● ●
3. Protect stored cardholder data.	●	●	
4. Encrypt transmission of cardholder data across open, public networks.			● ●
5. Use and regularly update anti-virus software or programs.		●	●
6. Develop and maintain secure systems and applications.			● ●
7. Restrict access to cardholder data by business need to know.			● ●
8. Assign a unique ID to each person with computer access.			● ●
9. Restrict physical access to cardholder data.	●	●	
10. Track and monitor all access to network resources and cardholder data.		●	●
11. Regularly test security systems and processes.		● ●	
12. Maintain a policy that addresses information security for employees and contractors.			● ●

Voltage SST Technology in Customer Implementations

A major global credit card processor

BUSINESS DRIVERS:

- Want to offer value-added PCI scope reduction services in e-commerce and tokenization
- Service offerings must work with merchant applications seamlessly

SITUATION:

- Disparate systems including Stratus VOS, HP/UX and HP NonStop across multiple data centers
- Solution must have one-to-one correspondence between token and card numbers at all times to avoid breaking merchant processes.
- In house database-driven tokenization difficult to scale; limited by performance; and had too much complexity to ensure token consistency

SOLUTION:

- Voltage SecureData with SST and Voltage SecureData Web™ proof-of-concept completed quickly; now in roll-out phase to merchants

A US airline

BUSINESS DRIVERS:

- Can't protect PCI Data
- High risk of data breach, brand damage
- Aggressive compliance deadlines

SITUATION:

- Remove e-commerce web servers from PCI scope
- Applications that accept payment data: e-commerce, call center, mobile devices in-flight
- Multiple programming languages for applications, data in Microsoft SQL server

SOLUTION:

- Voltage SST brought systems into compliance
- Took e-commerce web servers and mobile payment data out of PCI scope
- Up and running in 4 hours, scalable for planned growth to Level 1 status

A medium-sized e-commerce electronics retailer

BUSINESS DRIVERS:

- Not compliant due to new requirements in PCI DSS 2.0; need to get compliant quickly
- Minimize audit scope and PCI footprint for simple compliance process

SITUATION:

- Current security controls left systems in PCI scope and non-compliant
- All Microsoft environments with three major applications handling tokens: POS, contact center, and e-commerce

SOLUTION:

- Voltage SecureData with SST removed all systems from PCI scope, with higher security and audit scope reduction compared to other solutions
- Up and running in one day, with annual key rotation taking only five minutes
- Easily integrated with their all-Microsoft (SQL Server, .NET) environment

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**.

v02-22-2013