

Neutralize data breaches and deliver rapid PCI DSS compliance

HPE Secure Stateless Tokenization (SST) on HPE NonStop



HPE SST Difference

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

Data breaches are everywhere

Cyber criminals have proved adept at thwarting existing IT defenses and exploiting weak links in the payments ecosystem. Merchants, enterprises, e-commerce businesses and service providers face severe, ongoing challenges securing payment card data from capture through the transaction lifecycle. Businesses are also under pressure to achieve scope and cost-reduction goals in meeting compliance mandates such as the Payment Card Industry Data Security Standard (PCI DSS).

Tokenization, which is used as a way of replacing credit card numbers with randomly generated replacement values, is one of the data protection and audit scope reduction methods recommended by the PCI DSS.

By tokenizing payment card data, the scope of the PCI audit and cardholder data environment is limited because the storage of payment cards is being substituted by tokens. The footprint for attacks shrinks accordingly because token data is useless if stolen.

Tokenization has emerged as a powerful technique for removing live data from systems while achieving PCI scope reduction.

Your breakthrough tokenization solution

To help you protect your data, HPE Security—Data Security delivers the SST Solution running on HPE NonStop servers, the platform of choice for payments processing for more than 40 years. HPE Secure Stateless Tokenization (SST) is an advanced, patent-pending, proven data security technology. HPE SST provides data-centric protection, so data is protected in use and in transit, across multi-platform ecosystems including payment devices, gateways, data stores, and applications.

As a native, stateless tokenization solution on HPE NonStop, it eliminates the token database that is central to other tokenization solutions and removes the need to store cardholder data. Eliminating the token database significantly improves the speed, scalability,

Solution brief

security and manageability of the tokenization process. Every application handling the tokenized data, including backend applications such as fraud analysis and loyalty programs, may then be removed from PCI audit scope.

When deployed with XYGATE Data Protection (XDP), HPE SST can be implemented with no changes to your existing applications or databases. Support for Enscribe-based applications is available now from XYPRO. Contact your HPE NonStop Sales Representative to find the availability of HPE NonStop SQL/MP and SQL/MX supported versions.

HPE SST and HPE NonStop solution advantage

• Reduced compliance audit scope

HPE SST technology is format-preserving, which means tokens can be configured to exactly match the format of the original data, such as a credit card number (between 12 and 19 digits) or to substitute alpha characters for certain digits (enabling tokens to be immediately identified as tokens). This simplifies and reduces audit scope and costs, accelerates compliance initiatives and mitigates the risk of breach of highly sensitive data.

• Neutralize data breaches

By eliminating token databases, HPE SST eliminates stored high-value sensitive customer data like credit card numbers that could be targeted through an attack.

• Maintain current business process

PCI DSS allows certain digits of a credit card number to remain “in the clear”—normally the first six digits or the last four. HPE SST optionally preserves these digits, allowing many business processes to work with tokens without the need to de-tokenize or require any changes to the existing process.

• Advanced technology

HPE SST on HPE NonStop allows fully native tokenization without requiring separate Web Service calls, permitting high-speed operations. A single operation can now be used to both decrypt and tokenize incoming sensitive data, for example, Primary Account Number (PAN) data. This single operation reduces latency by eliminating the need to send tokenization requests to a separate server.

• HPE NonStop fundamentals

HPE SST technology on HPE NonStop assures high availability and throughput to support business processes. For transaction processors, including payment switches, tokenization service providers and card issuers, as well as enterprises and merchants, SST technology supports the business with high performance, payment processor-grade high availability and 100% data consistency. Scalability is linear, providing capacity for distribution of tokenization across geographies and systems, and predictable capacity increases for high-growth businesses and seasonal demand peaks.

• Cost savings you deserve

Optimizing the costs of IT operations is a key objective for every organization today. HPE NonStop servers have the lowest TCO in its class for complex, mission-critical application environments.

One solution for your data breach protection needs

HPE SST uses static, pre-generated tables containing random numbers created using a FIPS random number generator. Lookup tables with random numbers cannot be related back to sensitive data. Compared to legacy offbox tokenization systems, eliminating token databases from the HPE SST solution:

- Eliminates stored credit card numbers and removes the high-value sensitive data that could be targeted through an attack

- Eliminates the cost of external database hardware and software acquisition and/or licensing and replication software that a customer would have to maintain, external to HPE NonStop, and
- Means no database growth over time often a cause of performance degradation—and no replication and backup issues

For neutralizing security breaches

A critical component of any neutralizing data breach solution is the technology infrastructure. HPE SST Solution on HPE NonStop offers you the reliability, availability and scalability to combat data security breaches. HPE NonStop is designed specifically for the very highest availability levels. This means you can protect your business from data breaches continuously, a “must have” for all HPE NonStop and HPE Security—Data Security customers.

HPE NonStop. The platform for continuous business.

The proven reliability and virtually unlimited scalability of HPE NonStop, now with native HPE SST, will provide compelling business value for retailers and card-accepting enterprises that must secure sensitive customer credit card data, accelerate PCI compliance initiatives and achieve significant cost savings through PCI audit scope reduction.

What's next?

Contact your HPE NonStop or HPE Security—Data Security sales representative today and arrange for an assessment of the security of your sensitive data in your IT environment. Discover how HPE SST software running on the HPE NonStop platform can help you neutralize any data breaches.

Learn more at
hpe.com/us/en/servers/non-stop.html
hpe.com/software/datasecurityvoltage.com

HPE Security—Data Security

U.S. Tel: +1 (408) 886-3200

Support: +1 (866) 440-8917



Sign up for updates

★ Rate this document


**Hewlett Packard
Enterprise**

© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

4AA6-0815ENW, February 2016, Rev. 2