Hewlett Packard Enterprise

Data sheet

HPE Secure Stateless Tokenization (SST)

Delivers advanced protection for sensitive data

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 and processor-grade high availability, 100 percent data consistency, and linear scalability

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.

HPE Secure Stateless Tokenization (SST)

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

HPE SST is "stateless" because it eliminates the token database that is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. HPE SST has a unique 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

HPE SST 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 HPE SST the resulting tokens cannot be related back to the original sensitive data.

Additionally, HPE SST 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 HPE SST difference

Reduced compliance scope and costs
HPE 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.

- HPE SST 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 HPE 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, HPE SST is a secure, high-performance solution that meets carrier-grade and payment processor-grade high-availability requirements. It provides 100 percent 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.

HPE 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. HPE 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.

FEATURES	BENEFITS
No pre-requisites	Works with all platforms and languages; easily integrates with existing IT environments.
Fast deployment	HPE 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 percent consistent, one-to-one mapping between PAN input and token is provided by all servers in all data centers. HPE SST 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.
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. HPE SST dual controls are workflow-based, promoting efficiency as well as security.
Layered authentication and 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 detokenized PAN data. Enables control of scope by controlling exactly what applications are allowed to do: tokenize only, detokenize only, or partial de-tokenization with certain digits blocked.

FEATURES	BENEFITS
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	HPE SST is part of HPE SecureData Enterprise, delivering market-leading encryption, tokenization, data masking, and key management in a single unified architecture for enterprise-wide data protection.
PCI scope reduction	In addition to HPE SST, HPE SecureData also delivers technologies to substantially reduce PCI scope in use cases where tokenization doesn't fit: • HPE SecureData Web takes e-commerce Web servers up to 100 percent out of scope • HPE SecureData Payments POS solutions support PCI compliance at physical card-swipe devices

For information on Point-to-point Encryption (P2PE) to secure credit card data at card swipe, refer to the HPE SecureData Payments data sheet. For information on securing sensitive customer data from the ecommerce browser to the backend, refer to the HPE SecureData Web data sheet.

Learn more at

voltage.com
hpe.com/software/DataSecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-5576ENW, May 2016