WHITE PAPER

HPE SECUREDATA

HYPER SECURE STATELESS TOKENIZATION (SST)

BHAVNA SONDHI | CISA, QSA (P2PE), PA-QSA (P2PE)
NICK TRENC | CISA, CISSP, QSA, PA-QSA

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

HPE Security – Data Security engaged Coalfire Systems Inc. (Coalfire), a respected Payment Card Industry (PCI) Qualified Security Assessor (QSA) company, to conduct an independent technical assessment of their Secure Stateless Tokenization (SST™) technology. The goal of this assessment is to confirm that the technology would support a customer's overall PCI Data Security Standard (DSS) compliance efforts and help reduce the risk and scope of the cardholder data environment (CDE) for customers. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance assessment.

The SST assessment methodology was designed with two types of customers in mind:

1. The first type of customer includes merchants and consumer-facing enterprises (These are referred to collectively in this paper as merchants/enterprises) that handle credit card numbers and want to reduce risk and scope by bringing tokenization in-house. This gives the merchant or enterprise more flexibility since they are not bound to any 3rd party, such as a processor for facilitation of their tokenization services. Even running in their own data centers, the merchant/enterprise 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.
2. The second type of customer includes payment service providers such as transaction processors, payment switches, tokenization service providers, and merchant acquirers (these are referred to collectively in this paper as 'processors'). These customers are not primarily interested in their own 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, and thereby deliver significant audit scope reduction to those merchant customers as a primary benefit of the solution they provide. These tokens can also be for internal use by the payment service provider, as well as to provide tokenization service to merchants.

This paper contains the detailed analysis behind Coalfire's opinion, which can be summarized as follows: When properly implemented, SST technology would effectively promote PCI DSS compliance goals and reduce assessment scope for merchants and processors alike.

ABOUT HPE SECURITY – DATA SECURITY

HPE Security—Data Security drives leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, HPE Security – Data Security protects the world's largest brands and neutralizes breach impact by securing sensitive data-at-rest, in-motion, and in use. HPE SST is offered as part of the HPE SecureData platform that provides advanced encryption, tokenization, data masking, and key management to protect sensitive data across enterprise applications, data processing infrastructure, cloud, payment ecosystems, mission-critical transactions, storage, and Big Data platforms. HPE Security - Data Security, with its HPE SecureData platform, solves one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex data security use cases.

AUDIENCE

This report was written with two audiences in mind. The first includes customers who may be evaluating SST technology for use in their environments. As previously mentioned, this audience can be further segmented into merchants/enterprises and processors. The second is the audit community in general and QSAs in particular who need to understand how SST technology will affect their work as auditors.

ASSESSMENT SCOPE

The scope of this assessment was to conduct an independent review of HPE's SST technology. Specifically, HPE Security – Data Security wanted to accomplish the following:

- Confirm that SST technology would support a merchant's/consumer-facing enterprise's overall PCI DSS compliance efforts.
- Determine how SST would reduce the risk and assessment scope of a merchant's/enterprise's CDE.

In this report, Coalfire will explain SST technology at a high-level, delving into the technical aspects of the solution. Next, the report will assess the expected impact of the technology on audit scope using the PCI DSS. [1]

PCI COMPLIANCE SCOPE

There are many use cases where tokenization can be deployed, such as, tokenization to allow for routine business processes (such as repeat payments) to continue without re-use of card holder data. Tokens can also be pushed out of the Card Holder Data Environment (CDE) without necessarily bringing the destination into scope (subject to appropriate firewall rules). This allows for processes such as data analytics, fraud, etc., to be conducted without card holder data. These systems could then potentially be kept completely out of scope of PCI DSS..

In an example of service provider such as a merchant acquirer or payment processor, segment tokenization is often used as a mechanism for reducing the overall encryption footprint. Utilizing tokenization could be seen as a mechanism to centralize the encryption investment whilst having a large CDE that still requires cardholder data. Tokens can be used in the line of business applications without requiring encryption and, subject to access controls, can be used as an appropriate lookup token for requesting the full pan when needed. In some cases this can allow cloud compute resources to be consumed for data transformation operations that don't need the card holder data, and then the card holder data swapped in for the token at a later point in the payment operation.

Even when the solution is demonstrated to be effective and secure, there will always be some controls that must be assessed per the PCI standard (i.e. in scope). Yet the controls that are in-scope may be significantly reduced by a well-conceived and properly implemented tokenization solution. In addition, the reduction in risk of data compromise provided by a tokenization solution is extremely valuable, given the severe consequences that may result from data breach (including lost revenue, brand damage, negative publicity, legal actions, fines and more). However, contrary to common industry claims, the use of a tokenization solution does not completely eliminate compliance requirements.

EXECUTIVE SUMMARY OF FINDINGS

The following is a summary of key findings from Coalfire's review of the SST methodology.

1. The merchant audit applicable controls for PCI DSS are shown in Summary Chart of Potential Impact on Merchant Audit Applicable Controls Table (Page 16). A properly designed and deployed HPE SST solution has an impact on the assessment of 43 of PCI's 242 requirements for merchant environments.

[1] Unless otherwise stated, all references to both the PCI DSS and Payment Application Data Security Standard (PA-DSS) in this report are to version 3.2, published in 2016.

2. The SST solution can greatly reduce or even eliminate the need to store cardholder data, depending on, among other things, customer type and implementation scenario. This will result in:
    a. Ease of successfully meeting or reducing the applicability of PCI DSS requirements 3 and 9.
    b. Reduction in likelihood of cardholder data being exposed as a result of a security breach.
3. The SST approach potentially reduces the amount of cardholder data that must be transmitted over public and private networks. This will result in:
    a. Reduction in likelihood of cardholder data being exposed as a result of a security breach.
4. The SST approach potentially provides faster tokenization than conventional database-driven solutions, and it does so with greater security for cardholder data at rest and in transit.
5. The merchant or service provider environment cannot be fully out-of-scope for PCI DSS, but various controls can be non-applicable with use of the HPE SST solution.
6. PCI audit scope reduction can be maximized when tokenization is combined with Point-to-point Encryption (P2PE) from Point-of-Sale (POS) devices or from the browser window in e-commerce applications. These encryption solutions provide data security from the source at the point-of-capture, while the sensitive data is in transit, and through to the back-end where tokenization is employed. .

Organizations should perform risk assessments on all the system components connected to the CDE including the excluded system components to determine if they could impact the security of the CDE.

BEST PRACTICE GUIDANCE

Coalfire evaluated the SST methodology in light of current industry best practices. Relevant sources include, but are not limited to, the following:

1. PCI DSS Tokenization Guidelines, published by the PCI Standards Security Council in April, 2015
2. NIST Special Publication 800-38G, Recommendation for Block Cipher Modes of Operation: Methods for Format Preserving Encryption, published by NIST in March 2016

As of the release of this report update, these listed documents are the most current.

In addition to this white paper, customers could utilize various offerings provided by HPE in order to achieve further PCI DSS applicable controls reduction based on business needs.

1. HPE SecureData Mobile: *"*HPE SecureData Mobile PCI DSS Technical Assessment Whitepaper*"*, by Coalfire published in 2016
2. HPE SecureData Payments: *"*HPE SecureData Payments PCI DSS v3.2 Control Applicability Assessment Whitepaper*"*, by Coalfire published in 2016
3. HPE SecureData Web: *"*HPE SecureData Web PCI DSS Technical Assessment Whitepaper*"*, by Coalfire published in 2016

INTRODUCTION

Most tokenization solutions in the market require the merchant to store PANs in a tokenization database. In contrast, tokenization, when correctly implemented with HPE SST, eliminates the need for a merchant to store cardholder data in its environment. To process a transaction, a merchant sends the tokenization system a primary account number (PAN) in exchange for a unique, random number known as a token. The token is a 1-to-1 representation of the PAN that can be used for batch settlement, chargebacks, refunds, voids, and other post-authorization activities. The service provider does the necessary translation (PAN-to-token and vice versa) for the merchant, assuming responsibility for PAN storage and protection. The place where PAN and tokens are stored by the provider is called a vault. For obvious reasons, the tokenization vault is always in-scope for a PCI DSS assessment of the provider.

An essential attribute of tokenization is that it is non-reversible by any means other than the trusted 'host' facilitating infrastructure. That is, the original PAN can never be obtained by examining the token because there is no mathematical relationship between the two. The value is obtained through random or pseudorandom number generation; it is not a derivative of the account number.

CONVENTIONAL TOKENIZATION

In conventional tokenization, tokens are assigned to PAN through the use of an index. Picture the index as a simple, two-column table in which PAN is listed in one column and tokens are listed in the other. The association between the columns is purely random, as are the tokens themselves. For tokens which have been created previously, each row consists of a PAN-token pair. All other rows contain an empty slot for PAN and an unused token.

In the course of transaction processing, a merchant sends the PAN to a tokenization system (often a third-party service provider, but it can also be internal). That system places the PAN in the index at an available slot, thereby associating it with a pre-existing token. Then the token is sent back to the merchant where it can be stored for future use. Since the token is not considered cardholder data, it is not subject to PCI DSS controls[2]. When the merchant needs to perform post-authorization activities, it simply transmits the token back to the tokenization system, which in turn reverses the process to find the associated PAN and conducts the requested transaction on behalf of the merchant.

The solution is classified as stateful because the tokens in this scheme are in one of two states: in-use or not in-use. Each time a token is issued, the state of the system changes. To maintain integrity and avoid data loss, the state of the system (specifically, the token vault) must be constantly backed-up and/or replicated. Since replication is not instantaneous, multiple copies of the vault will be out of sync, resulting in cumbersome situations where multiple tokens are issued for the same PAN (often referred to as "collision"), or multiple PANs are associated with the same token.

HPE SECURE STATELESS TOKENIZATION

With SST technology, multiple tables of tokens are randomly generated one time for all possible PANs. This generation uses random numbers and a provably secure method. Each and every PAN in the numeric range has a token assigned to it for the life of the table(s). Since every token PAN is pre-associated with a token, the tables are stateless; they do not change. This eliminates the need to synchronize a database across data centers, or constantly back it up.

[2] Certain kinds of tokens may be used directly as payment instruments. That is, they can be monetized apart from the tokenization solution. The PCI SSC refers to these as "high value" tokens since they would have the same value to an attacker as the PAN they represent. For that reason, they may be in-scope for audit purposes.

Whereas stateful tokenization solutions typically use a database for indexing, stateless tables operate in primary memory. When a merchant transmits a PAN to the provider, tokenization and de-tokenization occur in RAM. There is no read/write operation to disk. This gives the SST approach a significant performance advantage over conventional solutions.

Merchants could either receive SST service from a third-party provider or may prefer to host the service themselves. The latter is particularly beneficial to larger merchants and consumer-facing enterprises that are geographically dispersed, process large volumes of transactions, and would like to limit or reduce the footprint of their PCI DSS scope. This is advantageous in a variety of ways. First, the merchant would have full control of their tokenization solution, and thus not be dependent on their payment processor to provide proprietary tokens. Second, SST technology manages and assigns tokens in ways that avoid almost all of the PCI scope impacts of traditional token solutions. Third, the HPE SecureData solution, with SST technology, ships as an all-inclusive virtual appliance, so there are no individual software components, application servers, or databases to be managed. When a merchant runs the SST technology in-house, fewer controls and protections are needed for the SST solution in-house than would be needed to secure a token vault and all the additional hardware and software, database management systems, etc. that are essential to conventional tokenization solutions.

With SST, Figure 1 depicts the dataflow diagram which also shows where the keys reside when SST tokenization is utilized.

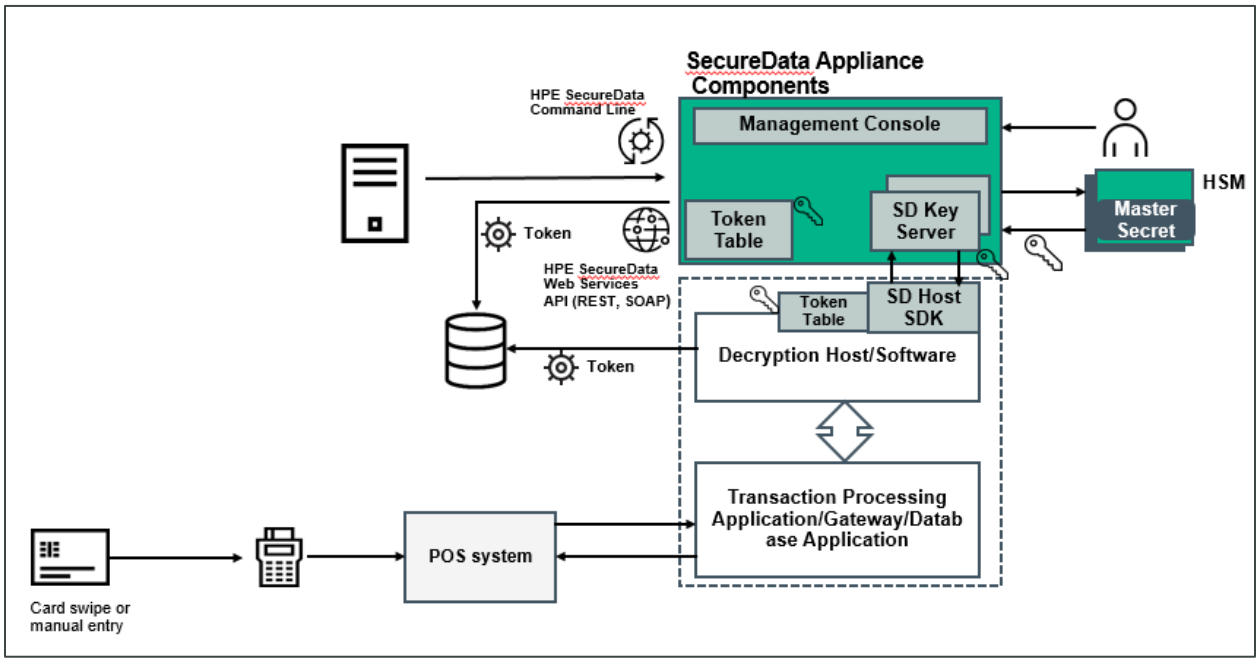


Figure 1: HPE SST End-to-End Data Security Flow Diagram

KEY NAME	USAGE	ALGORITHMS/ STRENGTH	KEY ROLLOVER	KEY SECURED BY
SST Key	Used to generate for base token	AES/FF1 mode/256 bit	Roll over is done when a new identity is generated	Derived from master secret as needed
SST Table File Key	Used to encrypt the SST table file	AES 256-bit	Roll over is done through management console at customer's control	Derived from the master secret and propagated to all registered hosts
Master Secret	HSM Master Secret	AES-256 bit	Use standard management console key group rollover (at customer's control)	Stored on HSM and secure backup smartcards

Hyper SST Implementations and Differences

The next generation of HPE SST, Hyper SST, provides the following improvements over the original version of HPE SST, and HPE recommends upgrading and using the new Hyper SST for these purposes.

1. Hyper SST includes NIST-standardized, FIPS-approved AES FF1 encryption (NIST SP-800-38G).
2. Code optimizations like control, data points and improved code structure have resulted in improved performance tokenization of an already high-performance solution.
3. Improved multi-threading capabilities deliver increased speed/performance over HPE SST and especially when compared to traditional database-centric tokenization solutions.

ASSESSMENT METHODOLOGY

The security of the SST method depends largely on the randomness of the tables[3] generated. If the values assigned to PANs are predictable, the tables might be reverse-engineered. Therefore, Coalfire examined decrypted binary samples of SST Feistel tables[4] to check for randomness. This was done using statistical tests developed by the National Institute of Standards and Technology (NIST) for the evaluation of random number generators[5]. The Feistel tables passed for monobit frequency (proportion of 0s and 1s for the entire sequence) and block frequency (proportion of 1s within M-bit blocks), as well as other statistical tests (Cumulative Sum and Binary Matrix Rank).

[3] There are two kinds of tables used: Permutation and Feistel. The number and kind of tables used in a given implementation depends on the length and composition of the PAN to be tokenized (more on this in the Design Review).

[4] Due to the way the samples were generated, only the Feistel tables could be tested with the NIST STS 2.1 software. The binary representation of SST permutation tables is not randomly distributed.

5 Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., & Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S. Department of Commerce, Technology Administration. (2010). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (Special Publication 800-22 Revision 1A). Retrieved from website: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Coalfire then conducted live technical testing of the SST technology itself. To accomplish this, Coalfire was provided a secure web interface and remote shell access to a running SST web service in the vendor's lab.

With a sufficient understanding of the SST methodology, Coalfire examined SST's impact on PCI DSS requirements. The scope impact was evaluated at a granular level looking at each control. The results were then summarized at a high-level by major requirement in the Summary Chart of Potential Impact on Merchant Audit Applicable Controls Table section.

DESIGN REVIEW

Secure Transmission

Prior to tokenization, a merchant using a tokenization service provider must transmit the PAN to that provider. In the case of an external provider accessed through the Internet, such transmission must be secure. Specifically, it must employ strong cryptography and security protocols (see PCI-DSS 4.1; PA-DSS 11.1). Sensitive account data cannot be sent in clear text over public networks.

For an internal provider (not accessed over the Internet), or for one that is using local SST technology, secure data transmission is optional. However, encryption is essential for organizations that want to reduce PCI DSS scope; otherwise, every host/segment that uses the service would be included in the CDE, resulting in a potentially massive expansion in scope.

Much of the technical analysis was conducted remotely using the vendor's lab environment. Throughout this phase, Coalfire observed that sessions were secured using Transport Layer Security (TLS) 1.2. At one point, an attempt was made to connect with Secure Sockets Layer (SSL) and TLS disabled on the client. As expected, the connection was refused by the vendor.

The screenshot image below (Figure 1) shows the vendor's response to an TLS 1.2 handshake from a Coalfire client. The acceptance of the older handshake is permissible so long as the response mandates a stronger cryptographic protocol (TLS 1.1, 1.2) as the vendor does, here. Therefore, the web service Coalfire used provided a PCI DSS compliant data transmission.

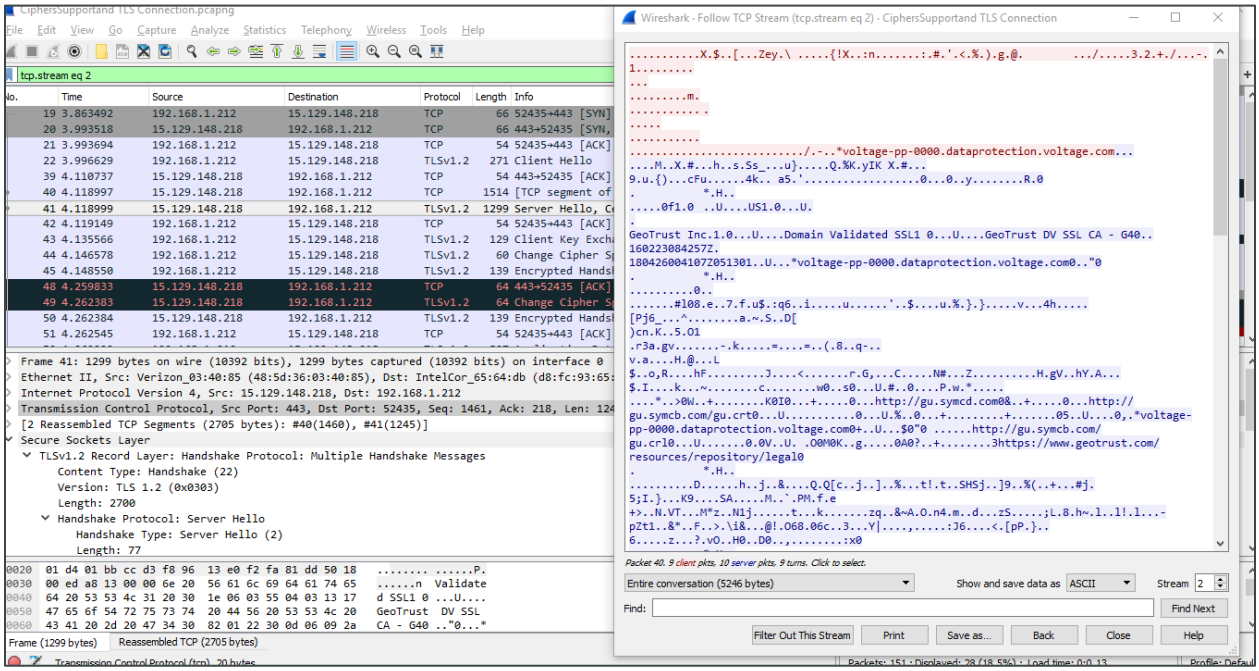
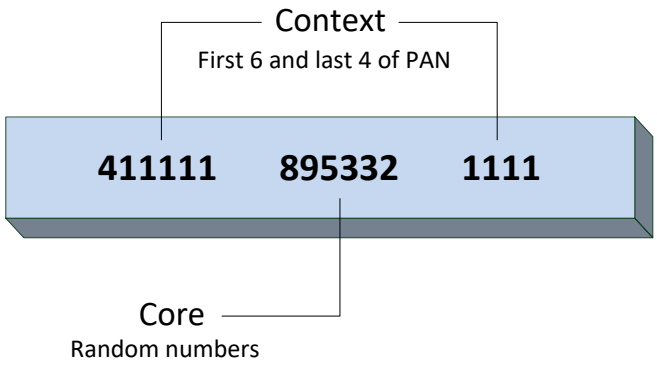


Figure 1: Secure Data Transmission

SST Token Anatomy

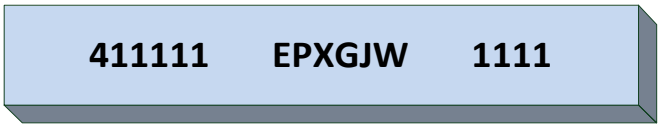
A token is a series of digits that can be divided into two types: context and core. Context digits are those that lead and/or trail within the token. Per PCI DSS v3.2 requirement section 3.4, no more than the first six and last four digits of the PAN may be used for context. The core digits, on the other hand, are randomly generated numbers taken from preexisting tables in memory.



The random digits selected for the core depend on the context digits. In this way, PANs with the same core digits will not be assigned to tokens that also have the same core digits. The length of a token and the number of core digits may change depending on the length of the PAN to be tokenized. At this point, the token is in an intermediate state.

Next, the core digits are encrypted using AES FF1 format preserving encryption (FPE). This further protects the values, as an attacker would need to obtain both the random tables and a decryption key to regenerate the input from a given token. The FPE step allows two different options for easily

distinguishing tokens from PANs. One is to only generate tokens that will specifically invalidate the Luhn algorithm in such a way that by inspection, tokens can be shown to not be live cardholder data. The other, if supported by the payment application, is to convert core digits to alpha-characters, an obviously tokenized format. The resulting token would look something like this:



The token is then ready for use. There is no way to reverse it and discover the associated account number, except by communication with the virtual appliance. Even though the core is encrypted, the plaintext is not PAN data; it is a string of purely random numbers (or letters). By definition, it is a truncated PAN and is therefore not considered cardholder data. Thus, it is not subject to PCI DSS requirements and can be considered out-of-scope for a PCI DSS assessment if it's segregated from the in-scope environment.

Table Generation

The generation of random number tables is perhaps the most technical and innovative aspect of the SST method. There are two types of tables involved: permutation and Feistel. As mentioned above, the SST method accommodates PAN of multiple lengths. While most credit cards use a 16-digit PAN, some use less (e.g., American Express with only 15) and others use more (e.g., Solo and Switch with up to 19). When a PAN's number of core digits (the digits needing protection after excluding the contextual digits) is seven or less, SST uses its permutation tables for tokenization.

Permutation tables are created using a random number generator (RNG) and a shuffling process. Take American Express, for example. Given 15 total digits in the PAN, subtract the first six and last four. That leaves five digits for the token core. Let N equal the number of core digits. The permutation table would have to contain values for all numbers in the range of $0…(10^5 – 1)$. That would be 100,000 unique numbers, generated randomly. Using a Knuth shuffle, this set of numbers is rearranged in a random, unbiased way so that each permutation is just as likely as every other.

What happens if more than seven core digits are required? Even if American Express is used, perhaps the merchant's back-end systems (e.g. accounting, customer loyalty) that would keep and/or use a card value, only retain the last four digits (not the first six). That would leave 11 core digits to adequately truncate the PAN, resulting in a table of almost 100 billion unique numbers, which is too large for a permutation table in memory.

In this case, a Feistel network is employed. The Feistel network is based on a series of tables created by the RNG, along with a randomization function that enables diversifying of the tables. Using multiple look-ups, these smaller tables work as one large "virtual table" for the purpose of tokenization.

ASSESSMENT METHODS

Coalfire conducted a technical analysis of SST technology by submitting test PAN through an Application Programming Interface (API) provided by the vendor in a remote lab. For each submission, the impact was observed on the network, the file system, and main memory. Broadly, the test environment consisted of:

1. A local *Java application* provided by the vendor that sends test PAN and receives tokens back from the tokenization server. This was installed on a Coalfire analysis platform, shown as a laptop in the diagram below.

2. The remote *tokenization server*. This is the server that accepts tokenization requests, performs token looks-ups, and responds with an associated token.

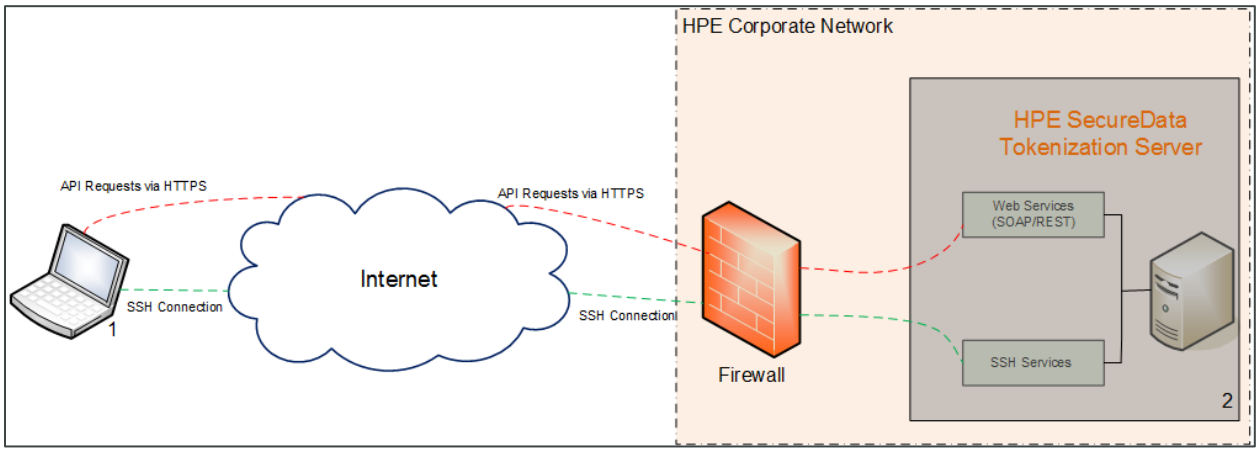


Figure 2: Test Environment

Token Exchange

The following examples illustrate the way in which the SST method works with PANs of different lengths. The number of leading and trailing PAN digits was selected using the Java application. Original and tokenized values are provided with the latter highlighted. (Note: These are not the only test PAN used by Coalfire during the assessment, these are samples out of the 6 other PANs tested.)

In the first example, three tokens that retain the first six and last four digits of PAN were requested from the server:

Data Length	Leading	Trailing	Example
All lengths	6	4	123456 EEEEEE 4321

Original	4012-0000-3333-0026
Tokenized	4012-0008-1254-0026
Original	5415-2444-4444-4444
Tokenized	5415-2437-7201-4444
Original	3759-644923-02967
Tokenized	3759-641994-32967

Next, three more tokens were requested. This time, only the last four digits of the PAN were retained:

Data Length	Leading	Trailing	Example
All lengths	0	4	EEEEEEEEEEEE 4321

Original	4012-0000-3333-0026
Tokenized	3482-9021-9523-0026

Original	5415-2444-4444-4444
Tokenized	8047-2651-7908-5454
Original	3759-644923-02967
Tokenized	6156-669191-22967

Additionally, tokenization was performed on all 16 digits of the PAN:

Original Cleartext PAN	4012-0000-3333-0026
Tokenized data	2056-5783-4001-5955

Original Cleartext PAN	5415-2444-4444-4444
Tokenized data	4197-2101-3487-9902

Original Cleartext PAN	3759-644923-02967
Tokenized data	7323-938019-43884

Finally, tokenization was performed on all 16 digits of the PAN with conversion to alphanumeric characters:

Original Cleartext PAN	4012-0000-3333-0026
Tokenized data	DEMH-FWYO-TIFH-ZEHO

Original Cleartext PAN	5415-2444-4444-4444
Tokenized data	IZGV-GZOD-IPHV-HZMY

Original Cleartext PAN	3759-644923-02967
Tokenized data	VSIX-DPOMUY-PRZXF

Network Traffic

As mentioned previously, all traffic between the Java application and the API service was secured using TLSv1.2 encryption. For this step, Coalfire used the Wireshark tool as depicted in Figure 3 below.

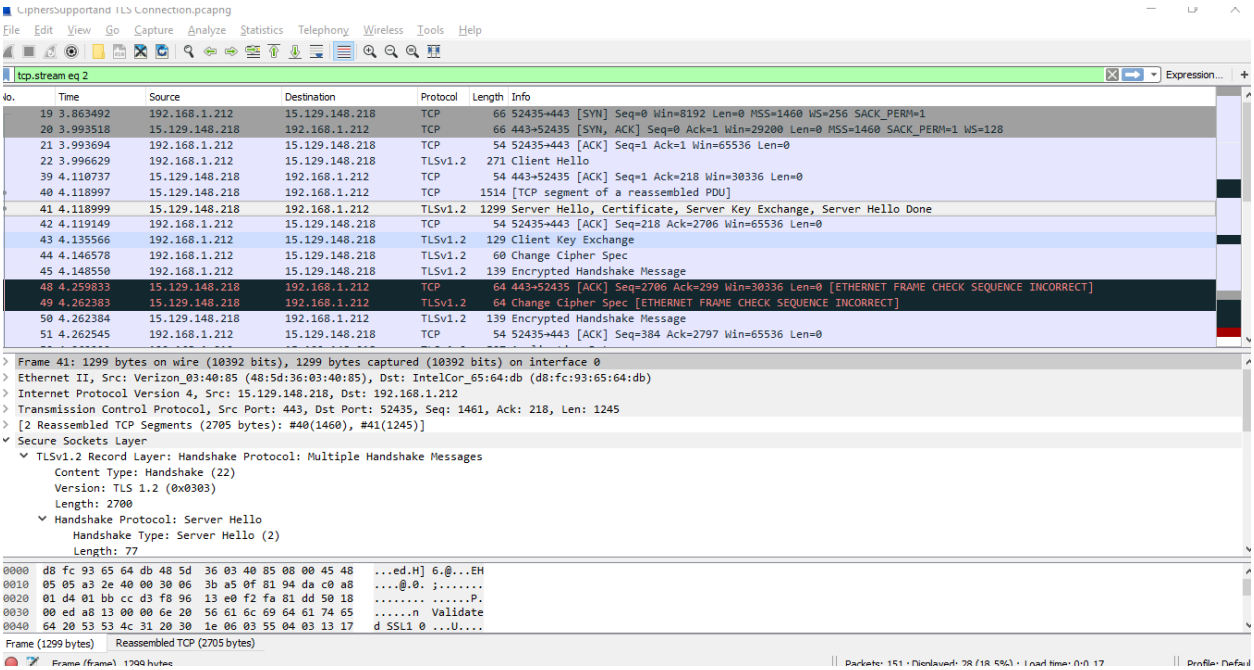


Figure 3: Wireshark traffic between Java application and API service secured over TLS 1.2

At no time was a submitted PAN found in clear text on the network. SST technology appears to provide adequate encryption of cardholder data in transit.

Penetration Testing

Coalfire attempted to exploit vulnerabilities on the web services using the Web Services Description Language (WSDL) file and attempted to modify a sample of requests employed by the web service using Burp Suite tool and SOAPUI Pro tool. No vulnerabilities were exploited or found during the penetration testing. Proper error response codes were received for the request attacks made on the server as depicted in Figure 4 below.

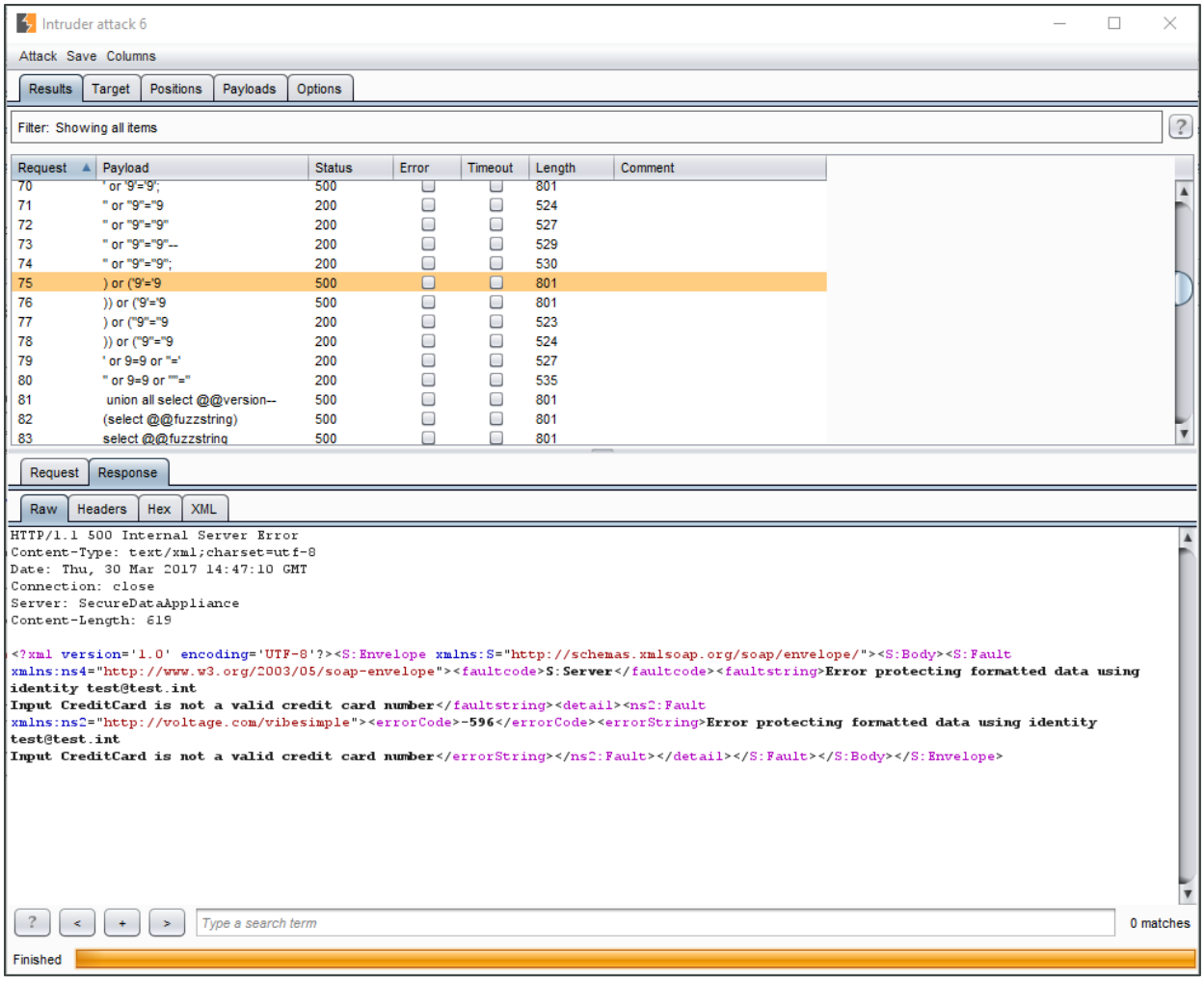


Figure 4: Sample attack request made for the credit card number field and response value using Burp Suite Tool

File System

At the same time traffic was being captured, Coalfire also monitored file system activity. This was done using the Linux audit facility (auditd). According to documentation provided by the vendor, token look-up occurs in memory. By monitoring files that hold encrypted tokenization table data, Coalfire confirmed that such look-ups did not involve access to those files.

Once enough PANs had been submitted, a bit-stream image was made of the file system and analyzed using FTK. A keyword search was conducted using both test PAN strings and regular expressions (regex). There were no search hits for test PANs in allocated or unallocated space, and there were no legitimate findings from regex. Thus, SST technology does not appear to "leak" account data onto the disk.

SUMMARY CHART OF POTENTIAL IMPACT ON MERCHANT AUDIT APPLICABLE CONTROLS TABLE

In the table below, the SST solution is evaluated against each of the major PCI DSS requirements. Scope reduction is categorized as major, moderate, or minor. With a major rating, a significant number of controls and/or the number of IT assets that must meet those controls could be removed from scope. A partial rating indicates that some controls and/or IT assets could be removed from scope of PCI DSS review. A minor rating indicates that few or no controls/assets are removed from scope of review during PCI DSS assessment by the SST technology.

Note that Applicable Control Reduction for this whitepaper here refers to the reduced number of system components required for review during PCI DSS assessment, the controls are always fully applicable within the merchant or service provider environment, however based on review of cardholder data environment, the segmentation and the applicable system components, there could be fewer components or assets applicable. The QSA working with the merchant or service provider company will be able to determine the controls that are fully or partially applicable for that organization during the PCI DSS assessment.

When considering the use of tokenization, the system components involved in acceptance of the PAN at the merchant location (card swipe or manual entry) always remain in scope for PCI DSS assessment.

PCI DSS REQUIREMENT SECTION	MAJOR APPLICABLE CONTROL REDUCTION	MODERATE APPLICABLE CONTROL REDUCTION	MINOR/NO APPLICABLE CONTROL REDUCTION
1			● ●
2			● ●
3	●	●	
4			● ●
5		● ●	
6			● ●
7			● ●
8			● ●
9	●		●
10			● ●
11		● ●	
12		●	●

● Merchant ● Processor

POTENTIAL IMPACT ON APPLICABLE CONTROLS TABLE

In this section, the SST methodology is evaluated against the DSS at a granular level. It separates the major requirements in the previous table, providing the anticipated scope impact on each control. Where appropriate, assessor comments are included in the far right column.

Key to Potential Impact on Applicable Controls Table

APPLICABLE CONTROL LEVEL	DESCRIPTION
✓	Control is Not Applicable for a properly and exclusively implemented solution based on HPE SST. The QSA should determine if the control applies to other sources of cardholder data. Note: Card swipe or manual entry at the merchant location is always in scope for PCI DSS assessment.
✓	Properly implemented, this solution reduces, but does not eliminate, the applicability of this control. The QSA should determine to what extent the control applies.
✓	Control is Applicable. Normal testing procedure should be used.
N/A	Control is Not Applicable for merchants as the requirement is either a requirement applicable to service provider or shared hosting provider.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1 Establish and implement firewall and router configuration standards	✓	✓	Perimeter firewalls and screening routers provide the first layer of defense against attacks originating from, or coming through, the public Internet. They also help prevent unwanted traffic and data from leaving internal networks. A merchant must ensure that it has robust filtering technologies and configuration standards along its perimeter.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.	✓	✓	
1.1.2 Current diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.	✓	✓	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks.	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	✓	✓	
1.1.5 Description of groups, roles, and responsibilities for management of network components.	✓	✓	
1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	✓	✓	
1.1.7 Requirement to review firewall and router rule sets at least every six months.	✓	✓	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	✓	✓	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	✓	✓	
1.2.2 Secure and synchronize router configuration files.	✓	✓	For a large transaction processor or service provider, the SST method would likely reduce the number of sites included in the CDE. Thus, the number or routers that are within scope may also decrease.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	✓	✓	
1.3 Prohibit direct public access between the Internet and any	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
system component in the cardholder data environment.			
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	✓	✓	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	✓	✓	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	✓	✓	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	✓	✓	
1.3.5 Permit only "established" connections into the network.	✓	✓	
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	✓	✓	This refers specifically to a database where cardholder data is stored. With SST, there is no such database.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	✓	✓	
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE.	✓	✓	
1.5 Ensure that security policies and operational procedures for managing firewalls are	✓	✓	Requirements concerning policies are always applicable.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
documented, in use, and known to all affected parties.			
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.	✓	✓	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	✓	✓	
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	✓	✓	With systems previously involved in the storage of CHD removed, there may be fewer configuration standards to maintain. For example, if a merchant formerly stored PAN in a database, and that was the only database instance in the CDE, there would no longer be a need to maintain a database configuration standard.
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	✓	✓	
2.2.2 Enable only necessary services, protocols, daemons,	✓	✓	When implementing the SST method, those services and protocols previously

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
etc., as required for the function of the system.			involved in cardholder data storage should be turned-off (disabled, blocked, etc.).
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	✓	✓	
2.2.4 Configure system security parameters to prevent misuse.	✓	✓	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	✓	✓	When implementing the SST method, those services and protocols previously involved in cardholder data storage should be turned-off (disabled, blocked, etc.).
2.3 Encrypt all non-console administrative access using strong cryptography.	✓	✓	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	✓	✓	
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	N/A	✓	Shared hosting providers are always subject to this requirement.
Protect Cardholder Data			
Requirement 3: Protect stored cardholder data			
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures, and processes that include at least the following for all cardholder data storage:	✓	✓	The primary benefit of the SST method is the removal of stored cardholder data from the merchant environment. When properly implemented, many of the controls in Requirement 3 would not apply to a merchant. For the processor/provider, some of them would apply to fewer systems.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
• **Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements** • **Processes for secure deletion of data when no longer needed** • **Specific retention requirements for cardholder data** • **A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention**			
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	✓	✓	For merchants who process card-present or card-not-present transactions, this is still fully applicable.
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	✓	✓	For merchants who process card-present or card-not-present transactions, this is still fully applicable.
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization.	✓	✓	For merchants who process card-present or card-not-present transactions, this is still fully applicable.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	✓	✓	For merchants who process card-present or card-not-present transactions, this is still fully applicable.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	✓	✓	Service providers and merchants may see a reduction in applicability since many systems will no longer have access to full PAN.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • **One-way hashes based on strong cryptography, (hash must be of the entire PAN)** • **Truncation (hashing cannot be used to replace the truncated segment of PAN)** • **Index tokens and pads (pads must be securely stored)** • **Strong cryptography with associated key-management processes and procedures**	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
general network login credentials). Decryption keys must not be associated with user accounts.			
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • **Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date** • **Description of the key usage for each key** • **Inventory of any HSMs and other SCDs used for key management**	N/A	✓	
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • **Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key** • **Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved**	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
point-of-interaction device) • **As at least two full-length key components or key shares, in accordance with an industry-accepted method**			
3.5.4 Store cryptographic keys in the fewest possible locations.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.1 Generation of strong cryptographic keys	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.2 Secure cryptographic key distribution	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.3 Secure cryptographic key storage	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.5 Retirement or replacement (for example, archiving, destruction,	✓	✓	This requirement will only apply to systems where full PAN information

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component) or keys are suspected of being compromised.			remains. This may be reduced at both the merchant and service provider level.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	✓	✓	This requirement will only apply to systems where full PAN information remains. This may be reduced at both the merchant and service provider level.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable. It is expected that the policy for cardholder data is that sensitive cardholder data is not stored or transmitted for service provider solutions.
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • **Only trusted keys and certificates are accepted.** • **The protocol in use only supports secure versions or configurations.**	✓	✓	Merchants would not be transmitting PAN site-to-site, so there may be far fewer instances of cardholder data being transmitted at all. Merchants would still be responsible, however, for securing transmission from card swipe/ manual entry location and between the tokenization system and the payment processor.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
• **The encryption strength is appropriate for the encryption methodology in use.** **Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.**			
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	✓	✓	For those merchants that utilize a wireless point-of-interaction (POI), this control would still apply.
4.2 Never send unprotected PANs by end user messaging technologies.	✓	✓	
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable. It is expected that the policy for cardholder data is that sensitive cardholder data is not stored or transmitted under any conditions.
	Maintain a Vulnerability Management Program		
	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs		
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	✓	✓	There would likely be a reduction in both merchant and processor assets that are subject to this control. Systems that do not have access to cardholder data (PAN) because of the SST solution may not be applicable for this requirement.
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	✓	✓	The SST solution does not impact the use of Anti-virus solutions themselves, just the applicability of system assets.
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate	✓	✓	There would likely be a reduction in both merchant and processor assets that are subject to this control. Systems that do not have access to cardholder data (PAN) because of the SST solution may not be applicable for this requirement

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.			
5.2 Ensure that all anti-virus mechanisms are maintained.	✓	✓	The SST solution does not impact the use of Anti-virus solutions themselves, just the applicability of system assets.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	✓	✓	
5.4: Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable. It is expected that the policy for cardholder data is that sensitive cardholder data is not stored or transmitted under any conditions.
Requirement 6: Develop and maintain secure systems and applications			
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	✓	✓	
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	✓	✓	There would likely be a reduction in both merchant and processor assets that are subject to this control.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
• In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices • Incorporating information security throughout the software-development life cycle			
6.3.1 Remove development, test, and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	✓	✓	
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines. • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
6.4 Follow change control processes and procedures for all changes to system components.	✓	✓	
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	✓	✓	
6.4.2 Separation of duties between development/test and production environments.	✓	✓	
6.4.3 Production data (live PANs) are not used for testing or development.	✓	✓	
6.4.4 Removal of test data and accounts from system components before the system becomes active/goes into production.	✓	✓	
6.4.5 Change control procedures must include the following: • **Documentation of impact** • **Documented change approval by authorized parties** • **Functionality testing to verify that the change does not adversely impact the security of the system** • **Back-out procedures**	✓	✓	
6.5 Address common coding vulnerabilities in software-development processes as follows: • **Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.** • **Develop applications based on secure coding guidelines.**	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	✓	✓	
6.5.2 Buffer overflows	✓	✓	
6.5.3 Insecure cryptographic storage	✓	✓	
6.5.4 Insecure communications	✓	✓	
6.5.5 Improper error handling	✓	✓	
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	✓	✓	
6.5.7 Cross-site scripting (XSS)	✓	✓	
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	✓	✓	
6.5.9 Cross-site request forgery (CSRF)	✓	✓	
6.5.10 Broken authentication and session management.	✓	✓	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • **Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least**	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
annually and after any changes. • **Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.**			
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	✓	✓	
Implement Strong Access Control Measures			
Requirement 7: Restrict access to cardholder data by business need to know			
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	✓	✓	Requirement 7 is geared specifically toward systems containing cardholder data, and the SST solution may reduce the number of systems in scope. Even so, merchants and service providers must implement these controls on systems within the CDE that do not store cardholder data.
7.1.1 Define access needs for each role, including: • **System components and data resources that each role needs to access for their job function** • **Level of privilege required (for example, user, administrator, etc.) for accessing resources.**	✓	✓	The sub-requirements around access control will fully apply to any remaining in-scope systems.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	✓	✓	
7.1.3 Assign access based on individual personnel's	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
job classification and function.			
7.1.4 Require documented approval by authorized parties specifying required privileges.	✓	✓	
7.2 Establish an access control system(s) for system components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	✓	✓	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable.
Requirement 8: Identify and authenticate access to system components			
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows	✓	✓	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	✓	✓	The SST solution may reduce the number of systems in scope (systems with cardholder data). Even so, merchants and service providers must implement these controls on systems within the CDE that do not store cardholder data.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	✓	✓	
8.1.3 Immediately revoke access for any terminated users.	✓	✓	
8.1.4 Remove/disable inactive user accounts within 90 days.	✓	✓	
8.1.5 Manage IDs used by third parties to access, support, or maintain system	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.			
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	✓	✓	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	✓	✓	
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	✓	✓	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	✓	✓	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	✓	✓	
8.2.3 Passwords/passphrases must meet the following: • **Require a minimum length of at least seven characters.** • **Contain both numeric and alphabetic characters.** • **Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.**	✓	✓	
8.2.4 Change user passwords/passphrases at least once every 90 days.	✓	✓	
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	✓	✓	
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	✓	✓	
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access	✓	✓	
8.3.2 Incorporate multi-factor authentication for all remote network access	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
(both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.			
8.4 Document and communicate authentication policies and procedures to all users including: • **Guidance on selecting strong authentication credentials.** • **Guidance for how users should protect their authentication credentials.** • **Instructions not to reuse previously used passwords.** • **Instructions to change passwords if there is any suspicion the password could be compromised.**	✓	✓	
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • **Generic user IDs are disabled or removed.** • **Shared user IDs do not exist for system administration and other critical functions.** • **Shared and generic user IDs are not used to administer any system components.**	✓	✓	
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a	N/A	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
password/phrase) for each customer.			
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • **Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.** • **Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.**	✓	✓	
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • **All user access to, user queries of, and user actions on databases are through programmatic methods.** • **Only database administrators have the ability to directly access or query databases.** • **Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).**	✓	✓	Under the SST solution, there should be no cardholder data repositories in the merchant environment and, as such, this requirement would not apply. For service providers, the number of cardholder data repositories may have been reduced and, subsequently, the number of in-scope data repositories that may apply to this requirement would also be reduced.
8.8 Ensure that security policies and operational	✓	✓	Requirements concerning policies are always applicable.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
procedures for identification and authentication are documented, in use, and known to all affected parties.			
Requirement 9: Restrict physical access to cardholder data			
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
			Transaction processors and service providers offering SST services will still need to validate these requirements.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • **Identifying onsite personnel and visitors (for example, assigning badges)** • **Changes to access requirements** • **Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).**	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.3 Control physical access for onsite personnel to sensitive areas as follows: • **Access must be authorized and based on individual job function.** • **Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.**	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
			not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.5 Physically secure all media.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
			not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.6.1 Classify media so the sensitivity of the data can be determined.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.7 Maintain strict control over the storage and accessibility of media.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
materials that are to be destroyed.			not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	✓	✓	Requirement 9 involves physical access to data or systems in the cardholder data environment. The merchant should still implement these controls as a matter of IT Security best practices. Nevertheless, the majority of these requirements would not apply since the merchant would have no systems that store cardholder data. Transaction processors and service providers offering SST services will still need to validate these requirements.
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	✓	N/A	Merchant inspection of devices is applicable. The encryption solution provider may have additional inspection procedures that are required of the merchant.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • **Make, model of device** • **Location of device (for example, the address of the site or facility where the device is located)** • **Device serial number or other method of unique identification.**	✓	N/A	
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	✓	N/A	
9.9.3 Provide training for personnel to be aware of attempted tampering or	✓	N/A	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
replacement of devices. Training should include the following: • **Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.** • **Do not install, replace, or return devices without verification.** • **Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).** • **Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).**			
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable.
	Regularly Monitor and Test Networks		
	Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Implement audit trails to link all access to system components to each individual user.	✓	✓	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	✓	✓	
10.2.1 All individual user accesses to cardholder data	✓	✓	The primary benefit of the SST method is the removal of cardholder data from the

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
			merchant environment. When properly implemented, logging of user access to cardholder data would not be required
10.2.2 All actions taken by any individual with root or administrative privileges	✓	✓	
10.2.3 Access to all audit trails	✓	✓	
10.2.4 Invalid logical access attempts	✓	✓	
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	✓	✓	
10.2.6 Initialization, stopping, or pausing of the audit logs	✓	✓	
10.2.7 Creation and deletion of system-level objects	✓	✓	
10.3 Record at least the following audit trail entries for all system components for each event:	✓	✓	
10.3.1 User identification	✓	✓	
10.3.2 Type of event	✓	✓	
10.3.3 Date and time	✓	✓	
10.3.4 Success or failure indication	✓	✓	
10.3.5 Origination of event	✓	✓	
10.3.6 Identity or name of affected data, system component, or resource.	✓	✓	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
acquiring, distributing, and storing time.			
10.4.1 Critical systems have the correct and consistent time.	✓	✓	
10.4.2 Time data is protected.	✓	✓	
10.4.3 Time settings are received from industry-accepted time sources.	✓	✓	
10.5 Secure audit trails so they cannot be altered.	✓	✓	
10.5.1 Limit viewing of audit trails to those with a job-related need.	✓	✓	
10.5.2 Protect audit trail files from unauthorized modifications.	✓	✓	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	✓	✓	
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	✓	✓	
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	✓	✓	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	✓	✓	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
example, online, archived, or restorable from backup).			
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • **Firewalls** • **IDS/IPS** • **FIM** • **Anti-virus** • **Physical access controls** • **Logical access controls** • **Audit logging mechanisms** • **Segmentation controls (if used)**	N/A	✓	
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	✓	✓	Requirements concerning policies are always applicable.
Requirement 11: Regularly test security systems and processes.			
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	✓	✓	
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall	✓	✓	The number of assets that would need to be included in these scans may be reduced for both merchants and service providers using the SST solution; however, the methods and processes in which these vulnerability scans must be conducted are not affected.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
rule modifications, product upgrades).			
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	✓	✓	The number of assets that would need to be included in these scans may be reduced for both merchants and service providers using the SST solution; however, the methods and processes in which these vulnerability scans must be conducted are not affected.
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	✓	✓	The number of assets that would need to be included in these scans may be reduced for both merchants and service providers using the SST solution; however, the methods and processes in which these vulnerability scans must be conducted are not affected.
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	✓	✓	The number of assets that would need to be included in these scans may be reduced for both merchants and service providers using the SST solution; however, the methods and processes in which these vulnerability scans must be conducted are not affected.
11.3 Implement a methodology for penetration testing that includes the following: • **Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115).** • **Includes coverage for the entire CDE perimeter and critical systems.** • **Includes testing from both inside and outside the network.** • **Includes testing to validate any segmentation and scope-reduction controls.**	✓	✓	With regard to coverage of the entire CDE perimeter and critical systems, use of the SST solution may reduce the number of assets that are applicable to this control; however, the methods and processes in which penetration testing occur are not affected.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
• Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.			
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	✓	✓	
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	✓	✓	
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	✓	✓	
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	✓	✓	If the number of in-scope systems is reduced through utilization of the SST solution, then the number of IDS systems needed to monitor traffic into and out of the in-scope environments may be reduced.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	✓	✓	If the number of in-scope systems is reduced through utilization of the SST solution, then the number of needed change-detection implementation should also be reduced.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	✓	✓	If the number of in-scope systems is reduced through utilization of the SST solution, then the number of needed change-detection implementation should also be reduced.
11.6 Ensure that security policies and operational procedures for security	✓	✓	Requirements concerning policies are always applicable.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
monitoring and testing are documented, in use, and known to all affected parties.			
Maintain an Information Security Policy			
	Requirement 12: Maintain a policy that addresses information security for all personnel.		
12.1 Establish, publish, maintain, and disseminate a security policy.	✓	✓	Requirements concerning policies are always applicable.
12.2 Implement a risk-assessment process that: • **Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),** • **Identifies critical assets, threats, and vulnerabilities, and** • **Results in a formal, documented analysis of risk.**	✓	✓	
12.3 Develop usage policies for critical technologies and define proper use of these technologies.	✓	✓	
12.3.1 Explicit approval by authorized parties	✓	✓	
12.3.2 Authentication for use of the technology	✓	✓	
12.3.3 A list of all such devices and personnel with access	✓	✓	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	✓	✓	
12.3.5 Acceptable uses of the technology	✓	✓	
12.3.6 Acceptable network locations for the technologies	✓	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
12.3.7 List of company-approved products	✓	✓	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	✓	✓	
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	✓	✓	
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	✓	✓	SST may eliminate this requirement for merchants and may significantly reduce applicability for service providers.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	✓	✓	
12.5 Assign to an individual or team the following information security management responsibilities.	✓	✓	
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	✓	✓	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.	✓	✓	SST will greatly reduce the number of merchant personnel who have access to cardholder data.

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.8.1 Maintain a list of service providers including a description of the service provided.	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by the entity.	✓	✓	The number of third-party organizations or service providers who have access to cardholder may be significantly reduced through the use of SST.
12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses	N/A	✓	

PCI DSS REQUIREMENT	MERCHANT IMPACT	PROCESSOR IMPACT	ASSESSOR COMMENTS
or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.			
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	✓	✓	
12.11: Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.	N/A	✓	Service providers must always meet this requirement.

REFERENCES

PCI SSC - Data Security Standard - https://www.pcisecuritystandards.org/documents/pci_dss_v3.pdf

PCI SSC - Data Security Standard- Payment Application Data Security Standard Program Guide, v3.2 - https://www.pcisecuritystandards.org/documents/PA-DSS_v3-2.pdf

PCI SSC – Tokenization Product Security Guidelines
https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf

CONCLUSION

As with conventional tokenization, the primary benefit of the SST method for merchants is the removal of cardholder data from the merchant environment. In a 2015 study on PCI compliance, Verizon [6] discovered that 62% of organizations were able to meet Requirement 3 of the PCI DSS (versus 44% in 2013). Around 38% of companies still fail to secure stored cardholder data. The protection of that data is one of the most difficult requirements to satisfy.

By replacing the conventional storage of cardholder data with SST technology, merchants could achieve significant scope reduction in several PCI DSS Requirement areas. Scope or control applicability reductions may also apply for the processor. This is mainly due to the decreased number of in-scope assets to which certain controls apply.

The tokenization tables at the heart of the SST approach have been found to be sufficiently random and unpredictable, and the algorithms that employ them are well-conceived. The SST method provides a more advanced methodology to PAN tokenization. By removing the database and essentially eliminating disk

6 Verizon 2015 PCI Compliance Report, Retrieved from website: http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

I/O, performance is increased over conventional tokenization solutions, and the high-value target of a token database that stores PANs is eliminated.

Typically, performance and security move in opposite directions, but not in this case. The overall security of the tokenization process is enhanced with SST. In a conventional indexed solution, compromise of the vault is a compromise of live PANs. In the SST method, there is no PAN storage. A complex series of tables in volatile memory hold pre-assigned tokens for every possible PAN. In order to use them, the attacker must also locate and compromise a decryption key. Assuming that a very skilled attacker could do this, the data would still be unusable. The attacker would only have the means of inputting PAN values and receiving tokens. He/she would need to possess live tokens that have been exchanged (e.g., by merchants) using those specific tables (which are often regenerated) and de-tokenize them to arrive at valid, live PANs. While technically not impossible, the significant effort required to compromise PANs in this solution makes it infeasible.

Though it is difficult to quantify the value in a chart, the costs of a data breach to a customer (monetary, damaged reputation, etc.) are tremendous. In the scramble to achieve compliance, the actual defense of information assets can often be overlooked. HPE's SST technology from HPE Security – Data Security avoids this pitfall by providing a secure, innovative, and robust solution. Therefore, it is Coalfire's opinion that HPE's Secure Stateless Tokenization technology, when properly implemented, would promote a merchant's PCI compliance goals, reduce the likelihood of cardholder data being exposed as a result of a security breach, and effectively reduce assessment scope for both merchants and processors alike.

ABOUT THE AUTHORS

Bhavna Sondhi | Senior Security Consultant | CISA, QSA (P2PE), PA-QSA (P2PE)

Bhavna Sondhi (bsasne@coalfire.com) brings over 10 years of software engineering and information security experience to the Application Validation team, leading extensive consulting and assessments engagements against the PCI-DSS and the PA-DSS standards within the USA, Europe, and Asia.

As a lead PA-QSA, Bhavna supports assessments for some of the largest payment software providers in the world, and her software engineering experience plays a vital part in ensuring the teams recognize the importance of secure code development and information security within their operational practices.

Nick Trenc | Principal Consultant – Practice Director | CISA, CISSP, QSA, PA-QSA

Nick Trenc (ntrenc@coalfire.com) is a Practice Director and Application Security Specialist with Coalfire Systems. Nick has several years of experience working as a QSA and PA-QSA helping clients develop systems and software for use in PCI DSS environments and has authored and spoken on multiple security topics including mobile security, application security, virtualization, cyber risk management, secure software development, and PCI DSS and PA-DSS compliance.

Published 28, July 2017.

ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com