Security Standards Council™

Standard: PCI Data Security Standard (PCI DSS)

Version: 2.0

Date: August 2011

Author: Scoping SIG, Tokenization Taskforce
PCI Security Standards Council

Information Supplement:
PCI DSS Tokenization Guidelines

SAMSUNG 1021

Table of Contents

1 Executive Summary ... 3

1.1 Objective ... 3
1.2 Intended Audience ... 3
1.3 Introduction to Tokenization ... 3

2 Tokenization Overview ... 5

2.1 Tokenization System Common Components ... 6
2.1.1 Token Generation ... 6
2.1.2 Token Mapping ... 7
2.1.3 Card Data Vault ... 7
2.1.4 Cryptographic Key Management ... 7
2.2 Tokenization Operations ... 8
2.3 Tokenization Security Considerations ... 10
2.3.1 Network Segmentation ... 10
2.3.2 Authentication ... 10
2.3.3 Monitoring ... 11
2.3.4 Token Distinguishability ... 11
2.3.5 PCI DSS Requirements ... 12
2.4 Tokenization Roles and Responsibilities ... 12
2.4.1 Tokenization Deployment Models ... 12
2.4.2 Merchant Responsibilities ... 14
2.4.3 TSP Responsibilities ... 15

3 PCI DSS Scoping Considerations ... 17

3.1 PCI DSS Scope for Tokenization ... 17
3.1.1 Scoping Principles ... 17
3.1.2 Out-of-Scope Considerations ... 18
3.2 Maximizing PCI DSS Scope Reduction ... 18

4 Additional Considerations ... 20

4.1 Tokens as Payment Instruments ... 20
4.2 Understanding the Risks ... 20

5 Conclusion ... 21

6 Acknowledgments ... 22

7 About the PCI Security Standards Council ... 23

1 Executive Summary

1.1 Objective

The purpose of this Information Supplement is to provide guidance for payment industry stakeholders when developing, evaluating, or implementing a tokenization solution, including how tokenization may impact Payment Card Industry Data Security Standard (PCI DSS) scope. This document provides supplemental guidance on the use of tokenization and does not replace or supersede PCI DSS requirements.

This document does not define the technical specifications or steps required to implement a tokenization solution, nor does it describe how to validate PCI DSS compliance for environments using tokenization. This document is not an endorsement for any specific technologies, products or services.

1.2 Intended Audience

This Information Supplement is intended for merchants that store, process, or transmit cardholder data and are seeking guidance on how implementing a tokenization solution may impact the scope of their compliance efforts with the (PCI DSS). Other payment industry stakeholders including payment processors, acquirers, service providers, assessors, and solution vendors may also find the information in this document useful.

1.3 Introduction to Tokenization

Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value called a ~~t~~oken." De-tokenization is the reverse process of redeeming a token for its associated PAN value. The security of an individual token relies predominantly on the infeasibility of determining the original PAN knowing only the surrogate value.

Depending on the particular implementation of a tokenization solution, tokens used within merchant systems and applications may not need the same level of security protection associated with the use of PAN. Storing tokens instead of PANs is one alternative that can help to reduce the amount of cardholder data in the environment, potentially reducing the merchant's effort to implement PCI DSS requirements.

The following key principles relate to the use of tokenization and its relationship to PCI DSS:

- Tokenization solutions do not eliminate the need to maintain and validate PCI DSS compliance, but they may simplify a merchant's validation efforts by reducing the number of system components for which PCI DSS requirements apply.
- Verifying the effectiveness of a tokenization implementation is necessary and includes confirming that PAN is not retrievable from any system component removed from the scope of PCI DSS.

- Tokenization systems and processes must be protected with strong security controls and monitoring to ensure the continued effectiveness of those controls.
- Tokenization solutions can vary greatly across different implementations, including differences in deployment models, tokenization and de-tokenization methods, technologies, and processes. Merchants considering the use of tokenization should perform a thorough evaluation and risk analysis to identify and document the unique characteristics of their particular implementation, including all interactions with payment card data and the particular tokenization systems and processes.

2 Tokenization Overview

One of the primary goals of a tokenization solution should be to replace sensitive PAN values with non-sensitive token values. For a token to be considered non-sensitive, and thus not require any security or protection, the token must have no value to an attacker.

Tokens come in many sizes and formats. Examples of some common token formats are included in the following table.

Table 1: Selected Examples of Token Formats*

PAN	Token	Comment
3124 005917 23387	7aF1Zx118523mw4cwl5x2	Token consists of alphabetic and numeric characters
4959 0059 0172 3389	72912911852318466312 9	Token consists of numeric characters only
5994 0059 0172 3383	599400x18523mw4cw3383	Token consists of truncated PAN (first 6, last 4 of PAN are retained) with alphabetic and numeric characters replacing middle digits.

**** Note:*** *This table provides a selection of examples only, and does not include all possible token formats.*

Tokens can be generally identified as either single-use or multi-use. A single-use token is typically used to represent a specific, single transaction. A multi-use token represents a specific PAN, and may be used to track an individual PAN across multiple transactions. A multi-use token always maps a particular PAN value to the same token value within the tokenization system. Determining whether single-use or multi-use tokens, or a combination of both, are appropriate for a particular merchant environment will depend on the merchant's specific business need for retaining tokens.

When evaluating a tokenization system, it is important to consider all elements of the overall tokenization solution. These include the technologies and mechanisms used to capture cardholder data and how a transaction progresses through the merchant environment, including transmission to the processor/acquirer. The tokenization solution should also address potential attack vectors against each component and provide the ability to confirm with confidence that associated risks are addressed.

The security and robustness of a particular tokenization system is reliant on many factors, including the configuration of the different components, the overall implementation, and the availability and functionality of security features for each solution.

2.1 Tokenization System Common Components

2.1.1 Token Generation

Token generation describes the process or method of creating a token. Common forms of token generation include but are not limited to:

- A mathematically reversible cryptographic function, based on a known strong cryptographic algorithm and strong cryptographic key (with a secure mode of operation and padding mechanism)
- A one-way non-reversible cryptographic function (e.g., a hash function with strong, secret salt)
- Assignment through an index function, sequence number or a randomly generated number (not mathematically derived from the PAN)

Note: *If a token is generated as a result of using a hash function, then it is relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of the PAN. Where hashed and truncated versions of the same PAN are present in the environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*

Whichever generation method is used, the recovery of the original PAN must not be computationally feasible knowing only the token or a number of tokens. This is true for both single-use and multi-use tokens. Additionally, access to multiple token-to-PAN pairs should not allow the ability to predict or determine other PAN values from knowledge of only tokens. Tokens should have no value if compromised or stolen, and should be unusable to an attacker if a system storing only tokens is compromised.

Note that where token generation is based on a reversible encryption method (where the token is mathematically derived from the original PAN through the use of an encryption algorithm and cryptographic key), the resultant token is an encrypted PAN, and may be subject to PCI DSS considerations in addition to those included in this document. The PCI SSC is further evaluating how these considerations may impact PCI DSS scope for reversible, encryption-based tokens.

Tokenization of sensitive authentication data (including magnetic stripe data or equivalent on a chip, CAV2 / CVC2 / CVV2 / CID data, and PINs/PIN blocks) is not permitted per PCI DSS Requirement 3.2.

2.1.2 Token Mapping

Token mapping is the process of assigning a token to the original PAN value. When a PAN is submitted for tokenization, the generated token and the original PAN are typically stored in the card-data vault. Token mapping provides the ability to retrieve either a particular PAN or a particular token, depending on how the solution is implemented and the type of request.

The ability to retrieve a PAN in exchange for its associated token should be restricted to specifically authorized individuals, applications, and/or systems. Any system component that can be used to retrieve PAN data would need to be protected according to PCI DSS.

2.1.3 Card Data Vault

In a tokenization system, the card data vault (or "data vault") is the central repository for PANs and tokens and is used by the token-mapping process. Wherever PAN data exists, it must be managed and protected in accordance with PCI DSS requirements.

Because it contains PANs as well as tokens, the data vault often presents the most attractive target for attackers. Compromise of the data vault could potentially result in the compromise of the entire tokenization system, and additional security controls above and beyond those required in PCI DSS may be warranted.

2.1.4 Cryptographic Key Management

Cryptographic key management defines the processes for creating, using, managing, and protecting cryptographic keys used for the protection of PAN data. Cryptographic keys must be managed and protected in accordance with PCI DSS requirements. In a tokenization solution, cryptographic key management applies to keys used for encrypting PAN in the card data vault, as well as any keys used in the generation of the tokens themselves.

Where token generation is based on the use of cryptographic keys, compromise of the keys could result in the compromise of all current and future tokens generated with those keys. Cryptographic keys used for token generation and de-tokenization should therefore not be available to any application, system, user, or process outside of the secure tokenization system.

2.2 Tokenization Operations

There are numerous ways to implement a tokenization solution. As a general principle, tokenization and de-tokenization operations should occur only within a clearly defined tokenization system that includes a process for approved applications to submit tokenization and de-tokenization requests. Figure 1 below shows an example of a tokenization process.

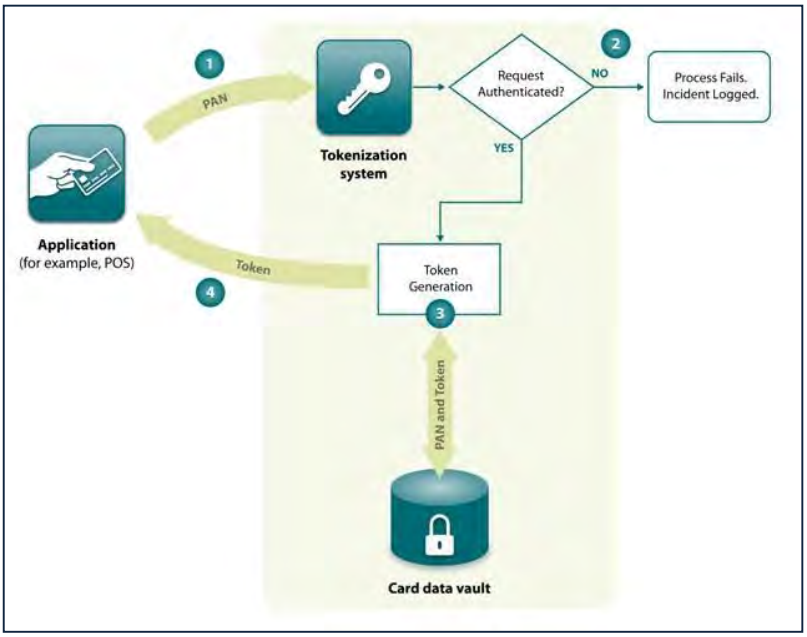

Figure 1: High-level example of a tokenization process

Note: *This is an example only that illustrates one possible tokenization process. Each solution should be individually evaluated to understand its particular processes and data flows.*

The steps illustrated in this example include:

1. A requesting application passes a PAN, along with necessary authentication information, to a tokenization system.
2. The tokenization system verifies the authentication information presented by the requesting application. If this check fails, the tokenization process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.
3. The tokenization system generates—or retrieves if already exists—a token associated to the PAN and records both to the card data vault, following PCI DSS requirements for PAN storage.
4. The tokenization system returns the token generated or retrieved in Step 3 to the requesting application.

De-tokenization typically reverses the steps from the tokenization process. An example of a de-tokenization process is sown in Figure 2 below.

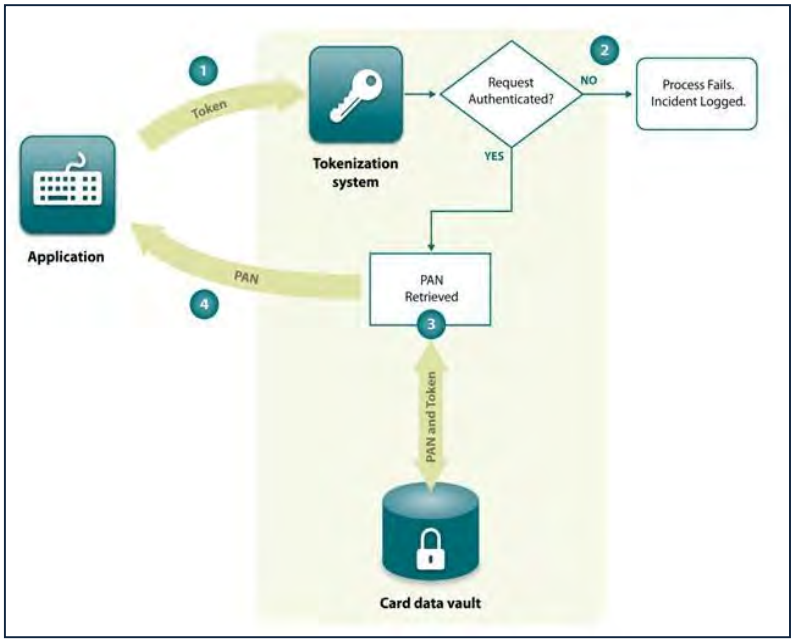

Figure 2: High-level example of a de-tokenization process

Note: *This is an example that illustrates only one possible de-tokenization process. Each solution should be individually evaluated to understand its particular processes and data flows.*

The steps illustrated in this example include:

1. The requesting application passes a token, along with necessary authentication information, to a tokenization system.
2. The tokenization system verifies the authentication information presented by the requesting application. If this check fails, the de-tokenization process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.
3. The tokenization system queries the card data vault for a record associated with the token, retrieves the PAN if found, and proceeds to Step 4. If no such token exists, the de-tokenization operation fails, and information is logged for monitoring.
4. The tokenization system returns the PAN value retrieved from the card data vault, if found, to the requesting application. If the PAN is not found, then an error message is returned.

Note: *If PAN is retrievable by the merchant, the merchant's environment will be in scope for PCI DSS. In order to minimize the presence of cardholder data in a particular merchant environment or network segment, the merchant would not need or have the ability to retrieve the PAN once the token has been generated.*

Some key considerations highlighted by these examples include:

1. Communications between the requesting application and the tokenization system must be secured to prevent interception or capture of cardholder data or token-to-PAN mapping information.
2. Strong authentication and access controls must exist for all access to the tokenization system, whether for tokenizing or de-tokenizing data, and authentication credentials must be secured from unauthorized access or use.
3. Security of the card data vault is critical for the security of the tokenization system as a whole, and must be secured at a minimum according to PCI DSS requirements to protect cardholder data.
4. All components within the tokenization system (for example, the token generation and mapping process, data vault, and cryptographic key management) must be located in a PCI DSS compliant environment.
5. Any system component with access to PAN data, or that has the ability to retrieve a PAN in exchange for a token, must be located in a PCI DSS compliant environment.

2.3 Tokenization Security Considerations

2.3.1 Network Segmentation

The tokenization system is considered part of an entity's cardholder data environment (CDE), and must be adequately segmented (isolated) from all networks not in scope for PCI DSS. Out-of-scope networks, applications, users, processes, and system components must not have access to authentication credentials that can be used to authenticate to the tokenization system or any part of the CDE.

2.3.2 Authentication

Only authenticated users and system components should be allowed access to the tokenization system and tokenization/de-tokenization processes. The authentication method should categorize all endpoints, including but not limited to applications, people, processes, and systems, to ensure the appropriate level of access is granted. In addition, consideration should be given to the following authentication items when evaluating a tokenization solution:

- **Identification** – Provides the required level of trust and assurance that the application, user, process, or system requesting access is uniquely identified.
- **Enrollment** – Establishes and ensures the uniqueness of identity during account provisioning.
- **Authentication** – Validates the identity of the application, user, process, or system at the time of a request.

- **Authorization** – Verifies the authenticated application, user, process, or system is permitted to submit a request, access a particular resource (such as data), or perform a particular activity.
- **Termination** – Removes or revokes the ability of an application, user, process, or system to successfully authenticate.
- **Maintenance** – Allows for ongoing management of accounts including but not limited to modification and termination.

2.3.3 Monitoring

The tokenization system should provide comprehensive and robust monitoring. All access to and actions within the tokenization system will need to be tracked, monitored, and logged in accordance with PCI DSS requirements. In addition, monitoring of the tokenization system should be sufficient to detect and alert personnel to any malfunctions, anomalies, and suspicious behavior that may indicate irregular token-to-PAN or PAN-to-token mapping requests or the presence of unauthorized activity within the tokenization process. Some tokenization systems can be configured to throttle or reject abnormal requests, reducing the potential exposure of unauthorized activity.

2.3.4 Token Distinguishability

The tokenization solution should include a mechanism for distinguishing between tokens and actual PANs. Distinguishability supports a merchant's ability to identify their sensitive data assets (in this case, PANs) so that appropriate security protections can be applied and verified. This also facilitates merchant and assessor efforts to validate the scope of the CDE as part of their annual PCI DSS review.

Without the ability to distinguish between a PAN and a token, the merchant or service provider may not realize that the tokenization system isn't functioning as intended. Additionally, PANs could be mistakenly identified as tokens, which can lead to mis-scoping of the CDE and the possibility that PANs are left unprotected and open to compromise.

Note that some tokens are designed to mimic the type and format of the original PANs, and it may not be possible for a human reviewer to distinguish between the two types of data. In this instance, a specific tool may need to be utilized or function performed to verify that an alleged token is actually a token and not a PAN.

The mechanism or method for distinguishing between tokens and PANs for a particular tokenization solution should be shared with the merchants using that solution, to allow merchants the ability to verify that their CDE has been accurately defined and scoped.

2.3.5 PCI DSS Requirements

Because the tokenization system stores, processes and/or transmits cardholder data, it must be installed, configured, and maintained in a PCI DSS compliant manner. Characteristics of a tokenization system that meets PCI DSS requirements include but are not limited to the following:

1. The tokenization system does not provide PAN in any response to any application, system, network, or user outside of the merchant's defined CDE.
2. All tokenization components are located on secure internal networks that are isolated from any untrusted and out-of-scope networks.
3. Only trusted communications are permitted in and out of the tokenization system environment.
4. The tokenization solution enforces strong cryptography and security protocols to safeguard cardholder data when stored and during transmission over open, public networks.
5. The tokenization solution implements strong access controls and authentication measures in accordance with PCI DSS Requirements 7 and 8.
6. The tokenization system components are designed to strict configuration standards and are protected from vulnerabilities.
7. The tokenization solution supports a mechanism for secure deletion of cardholder data as required by a data-retention policy.
8. The tokenization solution implements logging, monitoring, and alerting as appropriate to identify any suspicious activity and initiate response procedures.

2.4 Tokenization Roles and Responsibilities

The security considerations discussed in the previous section apply to the tokenization solution as a whole. Roles and responsibilities for a tokenization solution may be distributed between the various stakeholders—typically the merchant and tokenization service provider (TSP)—depending on its particular implementation or deployment model.

2.4.1 Tokenization Deployment Models

Examples of common deployments of a tokenization solution include the following:

- An on-premise or in-house solution that a merchant manages within its IT infrastructure
- An outsourced solution for which a merchant delegates management to a tokenization service provider outside of the merchant's infrastructure and control
- A hybrid solution that combines some on-premise components with some outsourced components

For an outsourced or hybrid tokenization solution, responsibility for ensuring that some system components comply with PCI DSS may be partially transferred from a merchant to a tokenization

service provider (TSP). Specifically, this would include components of the tokenization system that are managed by the service provider and are outside the control of the merchant.

As an example, if a merchant outsources their card data vault containing encrypted PANs to a TSP, the TSP would be responsible for ensuring that PCI DSS controls are applied and maintained in the environment where the vault is located. Merchants planning to use an outsourced or hybrid tokenization solution for their CDE should ensure that they thoroughly understand the details of the solution being offered. This should include performing a detailed assessment of the potential risks associated with using the solution. Additionally, it is crucial that both parties understand which controls and requirements are their responsibility, and which are the responsibility of the other party. Responsibilities for maintaining PCI DSS requirements, and any other controls that could impact the security of cardholder data, should be clearly defined between the two parties and documented in a formal agreement.

In an on-premise tokenization solution, the merchant maintains control over all components of the tokenization system. In this scenario, the merchant is fully responsible for complying with all applicable PCI DSS requirements. Merchants with on-premise solutions will also need to verify any segmentation controls that are implemented between their tokenization solution and any out-of-scope networks or systems. Before a system or network can be deemed out of scope for PCI DSS, it must first be verified that the system/network is not connected to the CDE and that it cannot retrieve or access PAN or other account data.

Figure 3 illustrates an example of how responsibilities may differ between merchant and TSP, depending on how the solution is deployed.

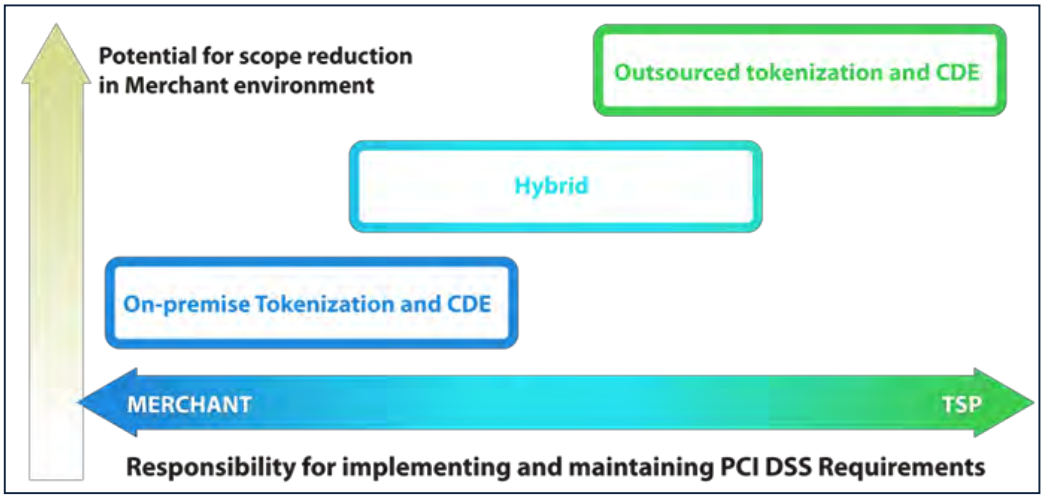

Figure 3: Example of how merchant and TSP responsibilities may be assigned for on-premise, hybrid, and outsourced solutions

Note: *Some PCI DSS requirements will apply to the merchant even when a tokenization solution is outsourced or hybrid. For example, PCI DSS controls apply wherever PAN is processed, stored, or transmitted—such as at the point of capture—as well as at any de-tokenization points. Additionally, the merchant is required to implement and maintain policies and procedures to manage service providers whenever cardholder data is shared.*

2.4.2 Merchant Responsibilities

The merchant has ultimate responsibility for the proper implementation of any tokenization solution they use, including its deployment and operation. Furthermore, the merchant is responsible for validation of its tokenization environment as part of their annual PCI DSS compliance assessment.

The merchant's level of responsibility for the tokenization solution can vary based on the extent to which the merchant manages it themselves or has outsourced some or all of the tokenization solution components. Depending on the tokenization solution implementation, the merchant's responsibilities may include but are not limited to some or all of the following:

- Ensure that the division of responsibility for protection of cardholder data is properly scoped and enforced.
- Verify the adequacy of any segmentation controls if these controls are not part of the supplied solution.
- Perform a risk assessment as part of their due diligence when selecting a tokenization service provider. Merchants should look for a provider with mature security processes that is capable of providing the required level of security as well as providing verification that the defined security controls are operational and effective.
- Ensure that proper contractual agreements are in place, with the tokenization service provider acknowledging that the service provider is responsible for the security of cardholder data processed, stored, and/or transmitted by the service provider.
- Maintain and implement policies and procedures to manage the tokenization service provider, including monitoring their PCI DSS compliance status at least annually.
- Verify that the solution supports and enforces the merchant's PCI DSS and security policy requirements, including but not limited to:
    - Data retention and disposal
    - Access control and authentication
    - Usage policies
    - Vulnerability management
    - Logging, monitoring and alerting

- Review logs of the merchant's interaction with the tokenization systems and processes on a regular basis to ensure that only users and system components authorized by the merchant have access to the tokenization/de-tokenization processes.
- Ensure that adequate incident response and disaster recovery plans are in place for the possibility of loss or compromise of the tokenization system. The following elements should be considered as part of these plans:
  - A risk analysis of all in-scope system components to determine the impact of a compromise.
  - A risk analysis for all out-of-scope system components that process, store, or transmit tokens to verify that they do not have access to the tokenization system or to PAN data, and to evaluate the impact of a compromise of tokenized data from those systems.
  - Strategies for remediation in the event of an incident or compromise. Examples may include but are not limited to rejecting de-tokenization requests from potentially compromised systems, reissuing tokens, and re-encrypting PANs in the data vault with new cryptographic keys.

Merchants using a hybrid or on-premise tokenization solution may be assuming the role of a TSP within their own organization, resulting in some or all of the TSP responsibilities (described below) also being applicable to the merchant.

2.4.3 TSP Responsibilities

The TSP has the overall responsibility for the design of an effective tokenization solution. Where a TSP manages one or more components of a tokenization solution on behalf of other merchants, additional responsibilities may include but are not limited to some or all of the following:

- Verify the security of all tokenization components under its control in accordance with PCI DSS requirements.
- Ensure that the tokenization solution supports the PCI DSS compliance of the TSP's customers. For example, the solution should provide secure transmission of cardholder data between the customer and the TSP, enforce secure authentication mechanisms for customer requests, implement customer access control policies, etc.
- Ensure that the tokenization solution supports the assignment of PCI DSS responsibilities between the TSP and their customers. For example, the solution should not return PANs to a customer without the customer's express permission and acknowledgement of how this action might affect the customer's responsibility for securing cardholder data and for validating PCI DSS controls.
- Ensure that responsibilities for maintaining and verifying PCI DSS controls are clearly defined between the customer and the TSP, and these responsibilities are documented in a tokenization service agreement.
- Develop and provide documentation to customer to assist in the proper deployment, implementation and use of the tokenization solution.

The TSP should clearly identify which PCI DSS requirements, system components, and services are covered by the TSP's PCI DSS compliance program. Any aspects of the solution not covered by the TSP are the responsibility of the merchant to manage and assess. The TSP should provide sufficient evidence and assurance that all processes and components under their control are PCI DSS compliant.

In summary, a TSP should ensure its tokenization solution meets all applicable PCI DSS requirements, supports their customers' PCI DSS compliance efforts, and helps to minimize their customers' need to store or access cardholder data.

3 PCI DSS Scoping Considerations

PCI DSS requirements apply to all system components within or connected to the CDE. The CDE is comprised of people, processes and technology that process, store, or transmit cardholder data or sensitive authentication data. To reduce the scope of a PCI DSS assessment, many organizations seek to minimize the number of system components that are included in or connected to the CDE. For example, network segmentation, which isolates systems that store, process or transmit cardholder data from those that do not, may reduce the scope of the CDE, and thus the scope of a PCI DSS assessment.

In general, tokenization can provide a model to centralize cardholder data storage and minimize the number of cardholder data occurrences in an environment. A properly implemented tokenization solution can reduce or remove the need for a merchant to retain PAN in their environment once the initial transaction has been processed. With adequate segmentation and process controls, a tokenization solution could help minimize the number of merchant system components that need to be protected according to PCI DSS.

3.1 PCI DSS Scope for Tokenization

All elements of the tokenization system and process, including de-tokenization and PAN storage, are considered part of the cardholder data environment (CDE) and are therefore in scope for PCI DSS. In addition, any system component or process with access to the tokenization system or the tokenization/de-tokenization process is considered in scope. System components that are adequately segmented (isolated) from the tokenization system and the CDE; and that store, process or transmit only tokens; and that do not store, process, or transmit any cardholder data or sensitive authentication data, may be considered outside of the CDE and possibly out of scope for PCI DSS. This section provides some high-level guidelines for scoping a tokenization solution for PCI DSS.

3.1.1 Scoping Principles

When scoping a tokenization environment for PCI DSS, the following general principles apply:

- All components of a tokenization system are considered part of the CDE and are always in scope since they store, process, and/or transmit cardholder data.
- System components that provide the ability to perform either of the following functions are in scope:
  - Generate a token in exchange for a PAN
  - Redeem a PAN in exchange for a token
- Any system component or process with access to the tokenization system or tokenization/de-tokenization processes is considered in scope as it is connected to the CDE.
- Any other system component located within or connected to the CDE, even if it does not perform tokenization or de-tokenization operations, is in scope.

3.1.2 Out-of-Scope Considerations

To be considered out of scope for PCI DSS, tokens, and the system components that store, process, and/or transmit only tokens would also need to meet following objectives:

- Recovery of the PAN value associated with a token must not be computationally feasible through knowledge of only the token, multiple tokens, or other token-to-PAN combinations.
- PAN cannot be retrieved even if the token and the systems it resides on are compromised.
- System components are segmented (isolated) from any application, system, process, or user with:
  - The ability to submit a de-tokenization request for that token and retrieve the PAN;
  - Access to the tokenization system, data vault, or cryptographic keys for that token;
  - Access to token input data or other information that can be used to de-tokenize or derive the PAN value from the token.
- System components are not connected to the tokenization system or processes, including the data vault, or cryptographic key storage.
- System components are not located within or connected to the CDE, nor do they have access to any authentication credentials that can be used to authenticate to any part of the CDE.
- System components do not store, process, or transmit cardholder data or sensitive authentication data through any other channel.
- System components that previously stored, processed, or transmitted cardholder data prior to implementation of the tokenization solution have been examined to ensure that all traces of cardholder data have been securely deleted.

3.2 Maximizing PCI DSS Scope Reduction

The key for merchants wishing to reduce their PCI DSS scope is to not store, process, or transmit cardholder data. Where there is a need to store cardholder data, retention should be limited to that which is required for business, legal, and/or regulatory purposes. If you don't need it, don't store it!

If tokens are used to replace PAN in the merchant environment, both the tokens and the systems they reside on will need to be evaluated to determine whether they require protection and should be in scope for PCI DSS. As described above, system components handling tokens that can be exchanged for a PAN or that can be de-tokenized to produce the PAN would be in scope. Any systems connected to the tokenization system or the CDE would also be in scope. To be considered out of scope for PCI DSS, both the tokens and the systems they reside on would need to have no value to an attacker attempting to retrieve PAN, nor should they in any way be able to influence the security of cardholder data or the CDE.

As part of their annual PCI DSS scope validation, merchants should review their use of tokens to ensure that cardholder data is not retrievable outside of the defined CDE. It should also be verified that tokens are being used as intended, and that any systems considered out of scope are adequately segmented from the CDE.

Additional recommendations for maximizing scope reduction for a merchant environment include the following:

- Replace PAN storage with tokens wherever possible;
- Limit existence of PAN to the point of capture and the card data vault;
- Minimize the number of system components that store, process, or transmit PAN prior to the PAN being tokenized;
- Ensure that PAN is not present in same environment as the tokens, outside of the card data vault;
- Ensure all PAN and other cardholder data is removed from source systems once it has been tokenized;
- Choose a solution that ensures PAN is not retrievable once a token has been issued; for example:
  - The tokenization solution does not permit a token to be exchanged for a PAN value.
  - The tokenization system does not provide PAN to the merchant in any response.
  - Once a token has been issued, all further transactions or processing (for example, refunds, chargeback, loyalty tracking, etc.) can be performed without the need for the merchant to retrieve or access the PAN.
- Enforce separation of duties such that token users and administrators do not have access to PAN at the point of capture or elsewhere;
- Combine an effective, secure tokenization solution with point-to-point encryption (P2PE), such that the only PANs in the environment are contained within a secure, PTS-approved point-of-interaction (POI) device.

Note: *If a token can be used to generate a transaction, additional security measures may be needed to protect against fraudulent use of the token. See "Tokens as Payment Instruments" in Section 4 for more information.*

4 Additional Considerations

4.1 Tokens as Payment Instruments

An important consideration when evaluating a tokenization solution is whether the token itself can be used in lieu of cardholder data to perform a transaction. Tokens that can be used as payment instruments (sometimes called ~~"h~~igh-value tokens") could potentially be ~~"m~~onetized" or used to generate fraudulent transactions, and may therefore have the same value to an attacker as the data they are intended to replace. Tokenization solutions which support these types of tokens should have additional controls in place to detect and prevent attempted fraudulent activities. Additionally, tokens that can be used to initiate a transaction might be in scope for PCI DSS, even if they cannot directly be used to retrieve PAN or other cardholder data; merchants should therefore consult with their acquirer and/or the Payment Brands directly to determine specific requirements for tokens that can be used as payment instruments.

4.2 Understanding the Risks

Tokenization is an evolving technology, and as with many evolving technologies, there is currently a lack of industry standards for implementing secure tokenization solutions. Organizations should carefully evaluate any solution before implementation to fully understand the potential impact to their CDE.

The architecture, implementation, and deployment of tokenization solutions can vary considerably, and the risks either created or mitigated by these systems are equally varied. Also, the advent of new attack vectors is likely to increase threats to tokenization systems. These factors mean that while a tokenization system may be secure against the best known attacks today, it may become vulnerable to attacks created in the future. Merchants and service providers should continue to monitor for new threats and potential risks to their existing use of tokenization.

When evaluating a tokenization solution, keep in mind that these solutions may introduce their own specific threats and security concerns. As with any evolving technology, care must be taken to understand the associated risks and avoid scenarios that may lead to cardholder data compromise.

5 Conclusion

Tokens and tokenization solutions can be implemented in numerous ways, and the security or process controls provided by one solution may not be suitable or applicable to another. Additionally, the assignment of roles and responsibilities may vary according to the particular solution or deployment method, and all entities involved should be aware of their obligations for maintaining security controls and protecting cardholder data.

The level of PCI DSS scope reduction offered by a tokenization solution will also need to be carefully evaluated for each implementation. For example, locations and flows of cardholder data, adequacy of segmentation, and controls around de-tokenization and mapping processes should be reviewed and verified to ensure proper scoping of the CDE and appropriate application of PCI DSS security requirements.

6 Acknowledgments

The PCI SSC would like to acknowledge the contribution of the Tokenization Taskforce, formerly part of the Scoping Special Interest Group (SIG), in the preparation of this document. The Tokenization Taskforce consists of representatives from the following organizations:

3DSI
Appsec
Barnes & Noble College Booksellers, LLC
BT Counterpane
Canadian Tire Corporation Limited
Canadian Tire Financial Services
Capita Group Plc
CipherOptics
Coalfire Systems
Cybersource
DSW Inc.
Elavon
FIS Global
Fishnet Security
Hallmark
HSBC
IBM
Illumis
Information Risk Management Plc
Ingenico
Intel
International Forecourt Standards Forum
John Lewis Plc
Key Innovations
Marks and Spencer
Merchant Link
MTXEPS Inc
Nelnet Business Solutions (formerly InfiNet)
Nettitude
Nike
Nubridges
Patrick Townsend Security Solutions
Paymetric Inc
PayPal
PCI SSC
Privity
Propay
Protegrity
PWC
Rogers Communications
RSA
S1 Corporation
Security Metrics
Semtek
Shift 4
Swedbank Card Services AB
Tesco
The Buckle Inc.
The College Board
T-Mobile
True Digital Security
Trustwave
US Bank
Verifone
Verizon
Verizon Business
VFC
Voltage
Witham Labs
WNCO

7 About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.