CyberSource®
the power of payment

CYBERSOURCE PAYMENT SECURITY COMPLIANCE

with PCI DSS Tokenization Guidelines

The PCI Security Standards Council has published guidelines on tokenization, providing all merchants who store, process, or transmit cardholder data with guidance on implementing a tokenization solution that will reduce the scope of compliance for PCI DSS (Payment Card Industry Data Security Standard).

To download the full PCI DSS Tokenization Guidelines, visit the PCI Security Standards Council website.

This document highlights how CyberSource Payment Security solutions align with the PCI DSS Tokenization Guidelines, sections 2 – 4, and how a merchant can reduce the time and resources it takes to validate with the PCI DSS. At CyberSource, our viewpoint has always been that taking sensitive payment data out of the merchant environment can provide effective security and reduce PCI compliance scope.

Table of Contents

© 2011 CyberSource, a Visa company. All rights reserved.

2. Tokenization Overview

2.1 Token Generation, Mapping, Data Vault, and Key Management

2.1.1 Token Generation

The PCI DSS Tokenization Guidelines list three common types of token generation:

- Mathematically reversible cryptographic function
- One-way non-reversible cryptographic function (e.g., hash function with strong, secret salt)
- Assignment through an index function, a sequence number or a randomly generated number (not mathematically derived from the PAN)

CyberSource generates its tokens using the third option, leveraging technology that produces tokens that cannot be mathematically reversed. As noted above, tokens generated using a hash function require additional controls to be in place to manage their security, presenting greater vulnerability in the event of a breach. CyberSource generates tokens using a proprietary index technology (or function), rather than a hash function. The resulting tokens are not derived from the PAN (Primary Account Number) in any way, though the token can retain the last four digits of the PAN for customer service and back office activities, and is backward compatible with legacy systems. Tokens provide zero monetary value and are worthless to hackers.

2.1.2 Token Mapping

"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."

CyberSource customers using tokenization always have the option of retrieving the PAN data associated with a token. The requested tokens are uploaded in a batch file to CyberSource and a merchant receives a file containing the PAN data.

However, as the Tokenization Guidelines states, any application or system on which PAN data is either transmitted or stored will be brought back in scope of the PCI DSS. Access to the PAN data should be restricted to authorized individuals, applications, and/or systems.

2.1.3 Card Data Vault

"Wherever PAN data exists, it must be managed and protected in accordance with PCI DSS requirements."

In adopting a hosted token solution, organizations can eliminate the need to have an on-site card data vault. Merchants will still retain a data vault that houses tokens, however that vault will not be in scope as long as PAN data is not stored within it.

2.1.4 Cryptographic Key Management

"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."

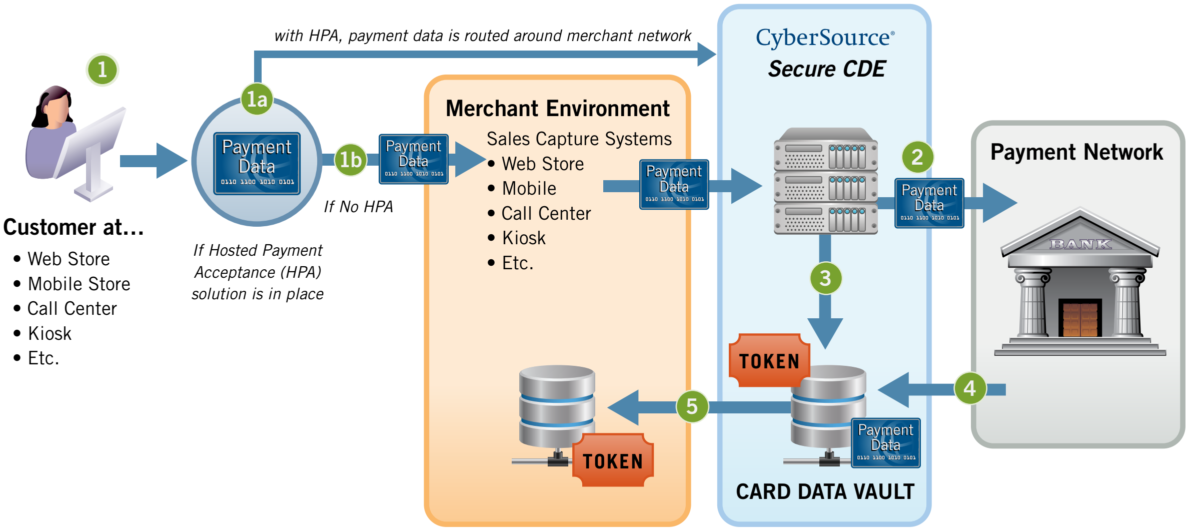
In eliminating token generation from their environment entirely, merchants have no need to manage encryption keys for tokenization.

© 2011 CyberSource, a Visa company. All rights reserved.

2.2 Tokenization Operations

> *"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."*

CyberSource's tokenization solution connects directly into merchant systems, providing a clearly defined CDE (cardholder data environment) that processes applications and creates tokens based on approved transactions.



The steps illustrated in this example include:

1. The customer enters their order information and PAN on a merchant's website.

   1a. If a Hosted Payment Acceptance solution is used, the payment data fields are hosted by CyberSource. PAN and transaction authentication information is routed directly to CyberSource via a secure HPA channel. (Non-PAN order data is routed directly to the merchant.)

   1b. If HPA is not being used, the PAN and transaction information are captured on merchant systems and transmitted to CyberSource.

2. CyberSource verifies the authentication information and sends the PAN to the payment network for authorization.
3. CyberSource also sends the PAN to the card data vault for secure storage.
4. The payment network provides the results of the authorization back to CyberSource.
5. CyberSource provides the generated token back to merchants, for storage in their database.

For de-tokenization, a merchant would submit a request through the CyberSource Business Center or make an API call to retrieve PAN data from CyberSource's secure card data vault, connecting directly to CyberSource. In exchange, a merchant would receive a response containing the PAN. However, merchant systems, applications, and personnel that have access to PAN data would be in scope.

© 2011 CyberSource, a Visa company. All rights reserved.

2.3 Tokenization Security Considerations

2.3.1 Network Segmentation

"The tokenization system… must be adequately segmented (isolated) from all other networks not in scope for PCI DSS."

The CyberSource Payment Tokenization solution resides completely outside of a merchant's CDE, and would be considered out of PCI DSS scope. However, if a merchant requests PAN retrieval, any of their networks where PAN data is transmitted or stored would be back in scope of the PCI DSS.

2.3.2 Authentication

"Only authenticated users and system components should be allowed access to the tokenization system and tokenization/de-tokenization processes."

Using CyberSource's Payment Tokenization and Hosted Payment Acceptance (HPA) solutions, merchants would have no access to PAN data, therefore the process of establishing and proving authentication is greatly reduced.

2.3.3 Monitoring

"All access to and actions within the tokenization system will need to be tracked, monitored, and logged in accordance with PCI DSS requirements."

With CyberSource Payment Tokenization, CyberSource is responsible for monitoring and tracking all activity.

2.3.4 Token Distinguishability

"The tokenization solution should include a mechanism for distinguishing between tokens and actual PANs."

As CyberSource tokens are randomly generated (to eliminate their mathematical reversal), they do not provide a characteristic distinguishing them from PANs. Merchants may add a field to their database to note the presence of a token.

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."

The use of CyberSource Payment Tokenization significantly reduces the effort required to comply with the PCI DSS, because the processing and storage of PANs are performed outside of a merchant's environment.

© 2011 CyberSource, a Visa company. All rights reserved.

2.3.5 PCI DSS Requirements (cont'd)

However, if a merchant is capturing a customer's PAN data on their own network and encrypting it before sending it to CyberSource, that portion of the network may be in scope. To further reduce PCI DSS scope, CyberSource Hosted Payment Acceptance solutions can transmit PAN data without it ever entering a merchant's environment.

2.3.5 PCI DSS Requirements	CyberSource
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.	Meets requirement. However, CyberSource provides PAN data if requested by the merchant (via either API or through the Business Center) and only by authorized personnel. Note: Re-introducing PAN data to the network places it back in scope.
2. All tokenization components are located on secure internal networks that are isolated from any untrusted and out-of-scope networks.	Meets requirement. All tokenization components are outside of the merchant's environment, so they would be automatically isolated from untrusted and out-of-scope networks.
3. Only trusted communications are permitted in and out of the tokenization system environment.	Meets requirement.
4. The tokenization solution enforces strong cryptography and security protocols to safeguard cardholder data when stored and during transmission over open, public networks.	Meets requirement when using tokenization in conjunction with HPA.
5. The tokenization solution implements strong access controls and authentication measures in accordance with PCI DSS Requirements 7 and 8.	Meets requirement.
6. The tokenization system components are designed to strict configuration standards and are protected from vulnerabilities.	Meets requirement.
7. The tokenization solution supports a mechanism for secure deletion of cardholder data as required by a data-retention policy.	Meets requirement by storing the PAN data as long as the merchant requires storage, but would ensure proper deletion of the data when requested by the merchant.
8. The tokenization solution implements logging, monitoring, and alerting as appropriate to identify any suspicious activity and initiate response procedures.	Meets requirement.

2.4 Roles and Responsibilities

2.4.1 Tokenization Deployment Models

The Tokenization Guidelines document states three common types of tokenization solution deployments:

- On-premise or in-house
- Outsourced solution with trusted service provider
- Hybrid solution combining on-premise and outsourced components

Per the guidelines, "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."

CyberSource is a tokenization service provider (TSP), providing an outsourced solution with all the necessary components to completely eliminate internal management of transaction processes. CyberSource Payment Tokenization greatly increases potential for scope reduction. Of course, merchants retain ownership of the PAN data and the option of requesting that it be returned (not recommended as this brings merchant networks back into PCI DSS scope).

© 2011 CyberSource, a Visa company. All rights reserved.

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."

CyberSource provides payment security solutions that can help merchants meet the responsibilities outlined in the Tokenization Guidelines.

2.4.2 Merchant Responsibilities	CyberSource
Ensure that the division of responsibility for protection of cardholder data is properly scoped and enforced.	Cardholder data is housed by CyberSource, a certified Level 1 service provider, and is fully protected in its PCI DSS-certified data centers in which security contingencies are enforced.
Verify the adequacy of any segmentation controls if these controls are not part of the supplied solution.	CyberSource's tokenization solution combined with HPA, is segmented out of the merchant environment.
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.	CyberSource can provide detailed verification that its security controls are operational, effective, and in full compliance with the PCI DSS requirements. CyberSource is a worldwide Level 1 PCI DSS-validated service provider and is listed on Visa's Global Registry of Service Providers.
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.	CyberSource retains the responsibility of protecting the cardholder data that it processes, stores, and transmits.
Maintain and implement policies and procedures to manage the tokenization service provider, including monitoring their PCI DSS compliance status at least annually.	CyberSource provides consistent communication with its customers, and verification of our ongoing PCI DSS compliance is readily available.
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	CyberSource supports and enforces the merchant's PCI DSS and security policy.
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.	CyberSource routinely monitors its systems and does not allow unauthorized personnel contact with any payment data, in adherence to the PCI DSS requirements.
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.	While merchants are responsible for implementing a risk analysis procedure for all in-scope systems in the event of a compromise, CyberSource provides an incident response and disaster recovery plan within its tokenization solution for all out-of-scope system components that process, store, or transmit tokens.

© 2011 CyberSource, a Visa company. All rights reserved.

2.4.3 TSP Responsibilities

"The TSP (tokenization service provider) has the overall responsibility for the design of an effective tokenization solution."

As the TSP, CyberSource is responsible for the design and effective use of the tokenization solution, as outlined in the Tokenization Guidelines.

2.4.3 Merchant Responsibilities	CyberSource
Verify the security of all tokenization components under its control in accordance with PCI DSS requirements.	CyberSource undergoes a PCI DSS service provider certification process annually to verify that all of its tokenization components are in accordance with the PCI DSS requirements.
Ensure that the tokenization solution supports the PCI DSS compliance of the TSP's customers.	CyberSource fully supports merchant compliance with PCI DSS requirements, when CyberSource Payment Tokenization is deployed exactly according to product specifications.
Ensure that the tokenization solution supports the assignment of PCI DSS responsibilities between the TSP and their customers.	CyberSource provides customers with a clear assignment of which PCI DSS that relate to each party.
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.	The service agreement between CyberSource and merchant clearly defines the responsibilities of both in terms of complying with PCI DSS controls.
Develop and provide documentation to customer to assist in the proper deployment, implementation and use of the tokenization solution.	All merchants receive full documentation on deploying, implementing and using CyberSource Payment Tokenization. In addition, if a customer is unsure about how to deploy a solution or needs additional guidance, CyberSource Professional Services can provide assistance.

3 PCI DSS Scoping Considerations

3.1 PCI DSS Scope for Tokenization

3.1.1 Scoping Principles

The Tokenization Guidelines provide general principles for determining the components that are in scope for PCI DSS. In general, the tokenization solution is considered part of the CDE, and therefore is in scope. Any system that connects or has access to the tokenization solution is also in scope.

CyberSource's Tokenization and HPA solutions reduce the footprint of a merchant's CDE by shifting the capture, transmission, processing, and storage of cardholder data outside its network, thereby reducing the components that would previously be considered within scope. However, if a merchant requests that the PAN be returned to their environment, systems on which it resides or is transmitted are considered in scope.

© 2011 CyberSource, a Visa company. All rights reserved.

3.1.2 Out-of-Scope Considerations

The tokenization guidelines also list objectives that the tokens and system components should achieve in order to be considered out of scope for PCI DSS.

CyberSource meets the out-of-scope considerations stipulated in the Tokenization Guidelines.

3.1.2 Out-of-Scope Considerations	CyberSource
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.	CyberSource utilizes a random token generation system that is not derived from the PAN, so the PAN value cannot be mathematically reversed.
PAN cannot be retrieved even if the token and the systems it resides on are compromised.	PAN cannot be retrieved using the tokens stored in the merchant's systems.
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.	CyberSource's tokenization system is housed outside the merchant's environment and is completely segmented from any internal application, systems, processes or users. Retrieval of the PAN (without express consent), access to the tokenization system, or access to input data used to de-tokenize the PAN is not feasible.
System components are not connected to the tokenization system or processes, including the data vault, or cryptographic key storage.	Merchant system components are segmented from CyberSource's tokenization solution, data vault, and encryption 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.	The merchant's CDE and CyberSource's tokenization solution are segmented from one another. Authentication is performed by connecting directly to CyberSource's payment processing engine.
System components do not store, process, or transmit cardholder data or sensitive authentication data through any other channel.	When deployed to product specifications for the transaction channels in question, the merchant will not capture, transmit, store, or process cardholder data when using CyberSource's Tokenization and HPA solutions.
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.	CyberSource will guide merchants to ensure that traces of cardholder data on their network have been securely deleted, but it is the responsibility of the merchant to confirm that the data no longer exists within their environment. Failure to do so may result in an in-scope determination by a QSA and is considered the merchant's liability.

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."

CyberSource Payment Security solutions provide merchants with the ability to significantly reduce PCI DSS scope by eliminating the presence of PAN data from their environment. Deploying Payment Tokenization and Hosted Payment Acceptance allows the merchant to replace PAN data with tokens, minimize the system components that process, store, or transmit PAN, and does not allow the retrieval of PAN data unless the merchant specifically requests it and understands the implications of that retrieval.

© 2011 CyberSource, a Visa company. All rights reserved.

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."

CyberSource tokens cannot be monetized. A hacker accessing a merchant's payment data vault comprised of tokens would be unable to process transactions using the tokens on file. Eliminating the ability of hackers to monetize tokens ensures that fraudulent activities will not occur, thereby reducing the merchant's exposure should a security breach occur.

4.2 Understanding the Risks

"Merchants and service providers should continue to monitor for new threats and potential risks to their existing use of tokenization."

To reduce the risk to merchants and ensure that PAN data is protected at all times, CyberSource implements the highest security controls available and updates these controls continuously.

CyberSource Payment Security Solutions

CyberSource Payment Security solutions fulfill the requirements specified in the PCI Security Council's PCI DSS Tokenization Guidelines. By using a TSP such as CyberSource, merchants can gain peace of mind that their customers' valuable cardholder data is protected, while significantly reducing their PCI DSS scope. When merchants shift the capture, transmission, and storage of PAN data to CyberSource, they can rest assured that it will be secured in a PCI DSS-certified data vault that is completely segmented from the merchant's internal systems.

For more information on CyberSource Payment Security solutions, please visit www.cybersource.com.

PCI DSS Tokenization Guidelines Document

To download the full PCI DSS Tokenization Guidelines document, visit the PCI Security Standards Council website.

PCI DSS Requirements

The PCI DSS requires that all merchants processing payment data either online or offline, must be in compliance with twelve requirements, listed here for your reference.

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measure	7. Restrict access to cardholder data by business need to know. 8. Assign a unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

© 2011 CyberSource, a Visa company. All rights reserved.

CyberSource®
the power of payment

CyberSource Americas

CyberSource Corporation HQ
Phone: +1 650-965-6000
Fax: +1 650-625-9145
Email: info@cybersource.com

CyberSource Europe

CyberSource Ltd
Phone: +44 (0) 118-929-4840
Fax: +44 (0) 870-460-1931
Email: uk@cybersource.com

CyberSource Japan

CyberSource KK (Japan)
Phone: +81 3-5774-7733
Fax: +81 3-5774-7732
Email: mail@cybersource.co.jp

CyberSource Asia Pacific

CYBS Singapore Pte Ltd
Phone: +65 6671-5010
Fax: +65 6671-5570
Email: ap_enquiries@cybersource.com

© 2011 CyberSource, a Visa company. All rights reserved.