

Merchant Link TransactionShield™ and TransactionVault™ Technical Review

Prepared for:

Merchant  Link

June 22, 2011

Project Lead and Report Author:

Bruce DeYoung, Director of Application Security Services

QA Review:

Kennet Westby, President and Co-Founder

Dan Fritsche, Managing Senior IT Auditor

01010101
01000001
01010101
01000001



Executive Summary

Merchants large and small continue to be plagued by data breaches caused by inadequate security controls or insecurely developed and deployed applications which leak or allow access to sensitive payment card data. Security professionals, service providers, application developers and hardware manufacturers are working across a number of security domains to address the data security needs of merchants. Two of the leading solutions intended to address the security of consumer credit card data in the merchant network are Point-to-Point Encryption (P2PE) and card data tokenization.

P2PE is intended to eliminate the availability of cleartext payment card data in transit through a merchant network by implementing data field encryption at (or as close to) card swipe or card data entry as possible. Once encrypted, sensitive payment card data is not decrypted until it arrives at a secured end-point, typically an acquirer, processor or gateway. In a well-designed P2PE solution, the merchant has no access to cryptographic keys or the decryption process and the encrypted data in transit to the processor network can significantly reduce risk of data breach and scope of PCI compliance requirements.

Payment card data tokenization is intended to eliminate the need to store such data after authorization in the merchant network by providing a unique card reference number, i.e. a *token*, in place of the original card data. Many merchants need card data for subsequent activities such as batch settlement, chargebacks, refunds, voids, etc. A well designed tokenization solution allows a merchant to store a non-cardholder data token which can be used for all subsequent transactional activities. The tokenization process is dependent upon a tokenization service provider which implements tokenization/detokenization, merchant cardholder data storage and token-to-cardholder-data mapping. A merchant which stores tokens as replacement reference values for the original cardholder data can greatly reduce the risk of data breach and scope of PCI requirements as well.

Merchant Link is a leading provider of cloud-based payment gateway and data security solutions and is listed as PCI DSS validated on Visa's Global Registry of Service Providers. Merchant Link engaged Coalfire Systems Inc. (Coalfire) as a respected Payment Card Industry (PCI) Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) company in good standing with the Payment Card Industry Security Standards Council (PCI SSC) to conduct an independent technical review of their P2PE and tokenization solutions, *TransactionShield* and *TransactionVault*, respectively. Coalfire conducted a technical review of *TransactionShield* and *TransactionVault* including design and architectural review, technical testing and forensic analysis, interviews, industry best practice alignment and review of existing compliance documentation.

In the absence of published compliance validation requirements for P2PE and card tokenization solutions from PCI SSC, Coalfire reviewed the *TransactionShield* and *TransactionVault* solutions following guidance provided in the currently available Visa Best Practice and PCI SSC Initial Roadmap documentation, including:

1. Visa Best Practices for Data Field Encryption published by VISA in October 2009.
2. Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance published by PCI SSC in October 5, 2010.
3. Visa Best Practices for Tokenization published by VISA in July 2010.

Additionally, since the implementation of a well-designed P2PE and tokenization solution can together significantly reduce PCI DSS scope for merchants, Coalfire reviewed the Merchant Link solution offerings against PCI DSS control requirements to determine where PCI DSS scope reduction may be realized.

This report has two intended audiences:

1. Merchants and service providers evaluating the Merchant Link *TransactionShield* and *TransactionVault* solutions for deployment in their payment card environment;
2. The QSA and Internal Audit community that is evaluating the Merchant Link *TransactionShield* and *TransactionVault* solutions or the impact of P2PE and card data tokenization on PCI DSS compliance in general on behalf of their merchants or service provider clients.

Summary of Findings

The relevant high-level findings from the technical review completed by Coalfire include:

1. *TransactionShield* is a P2PE solution that will leverage multiple encrypting *point of interaction* (POI) devices deployed in the merchant network with third party, integrated POS applications and a Merchant Link-hosted decryption process which can eliminate the transmittal of cleartext cardholder data through the merchant network.
2. *TransactionVault* is a tokenization solution hosted in Merchant Link's PCI DSS compliant data centers which can eliminate post authorization storage of cardholder data from a merchant's network.
3. *TransactionShield* is aligned with:
 - a. Visa Best Practices for Data Field Encryption published by VISA in October 2009.
 - b. Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance published by PCI SSC in October 5, 2010.
4. *TransactionVault* is aligned with:
 - a. Visa Best Practices for Tokenization guidance published by VISA in July 2010.
5. Implementation of the *TransactionShield* and *TransactionVault* solutions together can significantly reduce merchant PCI DSS scope. In particular, properly deployed, *TransactionShield* and *TransactionVault* can effectively remove merchant retail POS systems from the scope of PCI DSS by:
 - a. Capturing card data only via a *TransactionShield* integrated POS application and encrypting Point of Interaction (POI) device;
 - b. Strongly encrypting card data at the *TransactionShield* point of capture in a secure, restricted access, encrypting POI device, where the merchant has no ability to decrypt the card data;
 - c. Storing only card data tokens post authorization as returned by *TransactionVault*.