First Data TransArmor VeriFone Edition Abbreviated Technical Assessment White Paper

Prepared for:

October 1st, 2013

Dan Fritsche, CISSP, QSA (P2PE), PA-QSA (P2PE)
dfritsche@coalfiresystems.com

Overview

First Data engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Qualified Security Assessor Point to Point Encryption (QSA P2PE) company, to conduct an independent technical assessment of the *TransArmor VeriFone Edition* (TAVE)*, secured by RSA* security solution. Coalfire conducted assessment activities including technical testing, an architectural assessment, industry analysis, a compliance validation and peer review.

In this paper, Coalfire will describe how the *TransArmor VeriFone Edition* security solution can nearly eliminate the current risk of payment card data compromise within a merchant's retail environment and can dramatically reduce the scope of PCI DSS validation when properly deployed. This scope reduction will be based on evaluating the risk of each of the PCI DSS 2.0 requirements and how the TAVE security solution applies to each control within the context of the current PCI P2PE standards released in 2012. First Data could submit TransArmor VeriFone Edition to obtain a PCI P2PE listing, however the focus of this paper is to clarify how a merchant can benefit from TAVE even though it may not be a formally listed solution.

About TransArmor VeriFone Edition

TransArmor VeriFone Edition is a comprehensive, modular and flexible solution designed to provide merchants with strong encryption of payment card data from the point of capture to the point of decryption in First Data's secure data center. TAVE combines VeriFone's encryption methodology, VeriFone Total Protect (VTP) and Format Preserving Encryption (FPE), along with First Data's TransArmor tokenization technology.

The goals of the TransArmor VeriFone Edition solution are:

1. Reduce the risk of compromise to cardholder data throughout the entire transaction process, from point of entry through authorization and settlement.
2. Minimize the number and scope of controls that merchants must address for compliance to the Payment Card Industry (PCI) Data Security Standard (DSS).
3. Simplify and reduce costs associated for merchants with validation of PCI DSS compliance efforts.

TAVE helps shift the burden of protecting payment card data from the merchant to First Data using the latest encryption and tokenization technologies. This solution:

- Combines encryption and tokenization to protect cardholder data at every processing stage.
- Maintains all the merchant's business benefits of storing the payment cardholder data without the associated risk.
- Compliments Card Authentication technologies like EMV.

TAVE includes these high level components:

1. Merchant Point of Interaction (POI) – A VeriFone device encrypting cardholder data in hardware as it is collected.
2. First Data Switch – This includes First Data's Front End Authorization Platform (FEP) and STM handler for routing and processing capabilities. This is hosted by First Data in a PCI DSS compliant facility.
3. First Data Decryption and Tokenization – This includes the HSM, VeriShield Decryption Service (VSD) and TransArmor (TA) for tokenization. This is again hosted by First Data in a PCI DSS compliant facility.

This assessment included the above components in PCI compliant testing labs and focused on First Data's implementation of VeriFone's VTP encryption methodology, paired with TransArmor tokenization, to provide a secure encryption solution for merchants.

Assessment Scope

The scope of our assessment focused on the critical elements that validate the security and effectiveness of the security solution. Coalfire incorporated in-depth analysis of compliance fundamentals that are essential for evaluation by merchants, service providers and the QSA community. In addition, Coalfire utilized reviews and feedback obtained from members of the PCI community; however, the opinions and findings within this evaluation are solely those of Coalfire and do not represent any assessment findings, or opinions, from any other parties.

Although tokenization is part of the TAVE solution, this assessment focuses solely on how TAVE uses encryption and decryption technologies. The reader should gain an understanding on how TAVE can be understood and leveraged in the context of PCI DSS v2.0 and the current PCI P2PE standards released in 2012. Tokenization is relevant to protecting and reducing PCI DSS scope post-authorization for data at rest. For additional information regarding the value of Tokenization, please review the link below:

http://www.firstdata.com/downloads/thought-leadership/Value-of-Tokens-WP.pdf

Methodology

Coalfire has implemented industry best practices in our assessment and testing methodologies. Standard validation methods were used throughout the assessment. Coalfire conducted technical lab testing in both the Coalfire Lab located in Louisville, Colorado and the First Data lab in Omaha Nebraska. This included interviews, documentation review, transaction testing, encryption evaluation and forensic analysis.

Technical Security Assessment

Coalfire evaluated and tested the complete TransArmor VeriFone Edition security solution within the context of the applicable controls in the 6 domains as described in "Solution Requirements and Testing Procedures: Encryption, Decryption, and Key Management within Secure Cryptographic Devices Version 1.1" published by the PCI SSC in April 2012, as well as other related documents including updates to the standard. The evaluation included verification of encryption methods, key length, algorithms, key management methods, and physical and logical protection.

Summary Findings

The following are highlights of Coalfire's technical evaluation:

- A properly deployed *TransArmor VeriFone Edition* solution can provide significant risk reduction of data compromise and is one of the most effective data security controls available to merchants today.
- TAVE utilizes VeriFone's encryption in a secure manner that enables TAVE to provide the key benefits of using encryption to reduce a significant portion of PCI DSS controls remaining for a merchant to manage on a consistent basis.
- A merchant should have ownership rights to the decryption keys, but not have access to, or possession of these keys to achieve the greatest PCI DSS scope reduction.
- A merchant can dramatically reduce the PCI DSS controls they are responsible for validating in their retail and corporate environments if all electronic card data is captured at the POI in a *TransArmor VeriFone Edition* TRSM, the merchant is not capable of decrypting captured data, and decryption keys do not exist within their environment.
- A VeriFone PTS validated terminal should be the only point in a merchant retail environment that captures card data through any supported input method: swipe, manual, EMV or contactless. To achieve the greatest PCI DSS scope reduction, Coalfire and First Data recommend the use of a device with PTS 2.x with SRED or 3.x with SRED enabled.

Deployment Scenarios

The *TransArmor VeriFone Edition* solution can be used by many different types of merchants. The primary deployment difference will be which POI options a merchant needs.

Regardless of which POI devices are used, there are still several deployment assumptions that are required to achieve the full PCI DSS scope reduction for retail environments identified later in this white paper. The following assumptions are:

- Transaction locations only capture payment card data within a VeriFone PTS 3.x with SRED validated payment device.
- Payment applications and registers disable or procedurally restrict card swipe or card entry outside of the *TransArmor VeriFone Edition* payment device.
- No decryption capabilities of card data encrypted with *TransArmor VeriFone Edition* are accessible to the merchant.
- The merchant does not possess or have access to decryption keys in their retail or corporate environments.

- Chargeback and other customer support and payment research processes do not include or require access to the full primary account number. Most merchants will use First Data's TransArmor tokenization solution to remove card data from these processes.
- Public facing web applications for e-commerce or other payment transactional systems not using the *TransArmor VeriFone Edition* solution must be addressed with your QSA to determine PCI DSS requirements.

PCI DSS Scope Reduction Summary

The following summary chart provides a view of the impact to PCI DSS control requirements for a merchant's retail environment assuming TAVE has been properly implemented. Merchant environments can differ and it is important to work with your QSA to validate PCI DSS control validation scope reduction before making assumptions on scope reduction.

If a merchant has deployed TAVE in their environment, it is assumed that it is the only payment channel within the merchant's retail and corporate environments. Paper-based processes discussed within the justifications below would be in support of the TAVE payment channel only. All recommended risk reductions are based on the assumption that a QSA has fully validated that TAVE has been properly implemented in the merchant's environment.

Summary Chart of Merchant PCI DSS Scope Reduction

PCI DSS Area	Major Scope Reduction	Moderate Scope Reduction	Minor/No Scope Reduction
Section 1	**X**		
Section 2	**X**		
Section 3	**X**		
Section 4	**X**		
Section 5	**X**		
Section 6	**X**		
Section 7	**X**		
Section 8	**X**		
Section 9			**X**
Section 10	**X**		
Section 11	**X**		
Section 12			**X**

Legend:

- ***Major*** *– A significant number of controls are either removed from scope or a reduction in the number of IT assets requiring the controls*
- ***Moderate*** *– A reduced number of controls are required and a significant reduction in the number of IT assets requiring the controls*
- ***Minor*** *– Either no controls are removed from scope or minor impact to the scope of IT assets requiring the controls*

Assessor Comments

Our assessment scope put a significant focus on validating the PCI DSS scope reduction impact of the *TransArmor VeriFone Edition* solution. The *TAVE* solution can significantly reduce the risk of payment card data compromise for a merchant's retail environment. There can be very clear and dramatic reduction of the PCI DSS scope of validation with a properly deployed solution; however, ignoring the PCI DSS and security best practices, even if a merchant is out of scope for PCI DSS compliance validation, can introduce many other security or business continuity risks. Security and business risk mitigation should be any merchant's goal and focus for selecting security controls. The *TransArmor VeriFone Edition* solution can benefit merchants by helping reduce the cost of PCI DSS compliance validation and allow them to invest more of those resources into business risk mitigating controls.

With the release of the current PCI P2PE standard, merchants have an increased expectation to receive a more secure environment that utilizes the latest encryption technologies. First Data's *TransArmor VeriFone Edition* offering provides such an environment for several different types of merchants in light of a P2PE standard that may not fit every merchant.

Summary

TransArmor VeriFone Edition is a robust P2PE solution that, when implemented correctly, can be used by merchants to dramatically reduce both risk and scope for PCI DSS controls. First Data has integrated VeriFone's encryption properly and their back end decryption processes reside in a facility that has a current PCI DSS ROC in place. Merchants can use TAVE and this document to demonstrate how the technology works and enable QSAs or other interested parties to evaluate their proper implementation of TransArmor VeriFone Edition into their environment.

For more detailed information regarding the TransArmor VeriFone Edition solution, please review the detailed Technical Assessment which was published in concert with this summarized white paper.