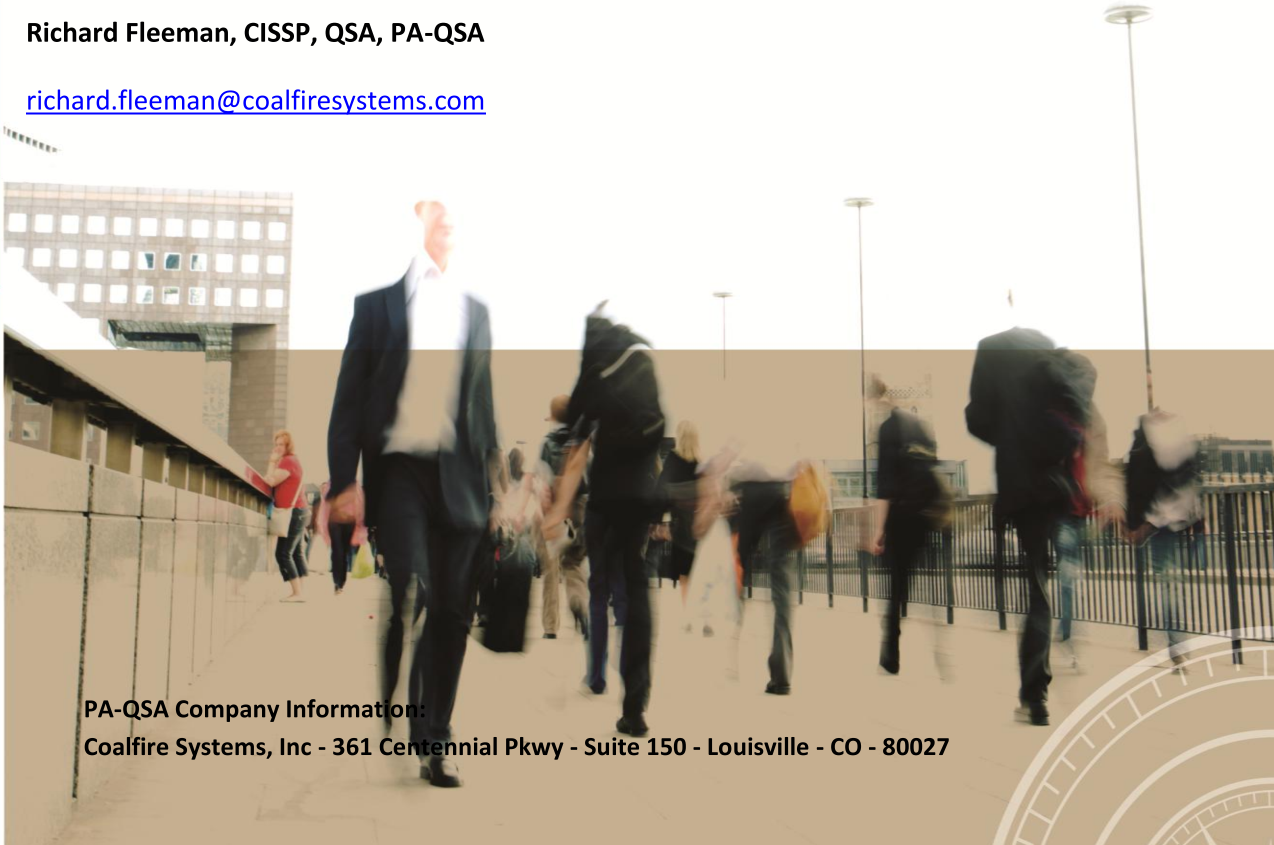
Datacap Systems – NETePay™ with dsiPDCX™ OOS PCI PA-DSS Out Of Scope Technical Assessment White Paper

July 6, 2011

Richard Fleeman, CISSP, QSA, PA-QSA

richard.fleeman@coalfiresystems.com



PA-QSA Company Information:
Coalfire Systems, Inc - 361 Centennial Pkwy - Suite 150 - Louisville - CO - 80027

Coalfire
IT Audit and Compliance

July 6, 2011

Datacap Systems, Inc.
Lee Morsillo, VP Engineering / Technology
100 New Britain Boulevard
Chalfont, PA 18914 USA

RE: Datacap NETePay™ with dsiPDCX™ Out of Scope Solution

Dear Lee,

This letter affirms that Coalfire Systems, Inc. has assessed the impact to a developer's PCI (PA-DSS) compliance when integrating the Datacap NETePay™ with dsiPDCX™ Out of Scope (OOS) solution with their POS software for handling of payment transactions.

Coalfire Systems, Inc. is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) approved by the PCI SSC to conduct PA-DSS & PCI-DSS assessments. The PA-DSS standard encompasses a set of criteria and key controls for the protection of cardholder data and sensitive information at the application level and applies to application vendors/developers.

The scope of the assessment focused on the critical elements of the Datacap NETePay™ with dsiPDCX™ OOS solution that may remove the scope of PCI PA-DSS compliance requirements from application vendors developing for the Datacap NETePay™ with dsiPDCX™ OOS solution. In addition, Coalfire incorporated in-depth analysis of compliance fundamentals that are essential for evaluation by merchants, service providers and the QSA community.

Based upon our analysis, Coalfire confirms that Datacap's NETePay™ with dsiPDCX™ OOS solution provides a complete solution to capture, process, transmit and/or store cardholder data as part of authorization or settlement. As a result, Point of Sale (POS) applications which integrate to Datacap's NETePay™ with dsiPDCX™ OOS solution may be removed from scope of PA-DSS compliance requirements as they are no longer "payment aware" and do not fit into the defined PA-DSS program of PCI SSC.

Sincerely yours,

Bruce DeYoung
Director, Application Security Services
bruce.deyoung@coalfiresystems.com
O: 303-554-6333 x7030

Contents

Executive Summary

Overview

Datacap Systems, Inc. (Datacap) engaged Coalfire Systems Inc. (Coalfire), as a respected Payment Card Industry (PCI) Payment Application – Qualified Security Assessor (PA-QSA) company, to conduct an independent technical assessment of the Datacap NETePay™ with dsiPDCX™ Out of Scope (OOS) solution. Coalfire conducted assessment activities including technical testing, architectural assessment, and compliance assessment.

In this paper, Coalfire will describe that the Datacap NETePay™ with dsiPDCX™ OOS solution can remove or keep an OS based Point of Sale (POS) system out of scope of the Payment Application – Data Security Standard (PA-DSS) with a properly integrated solution from Datacap.

About Datacap NETePay™ with dsiPDCX™ OOS

Datacap's NETePay™ with dsiPDCX™ OOS software option for OS based POS systems handles all card holder data during the authorization and settlement process, allowing POS developers to achieve an 'Out of Scope′ solution to major payment processors.

There are two deployment scenarios for Datacap's NETePay™ with dsiPDCX™ OOS solution:

1. OS based POS systems using the Datcap NETePay™ with dsiPDCX™ OOS with the Datacap PDC™ (Peripheral Device Controller) device with integrated MSR and a PCI PTS compliant device. In this deployment scenario, the NETePay™ with dsiPDCX™ OOS is responsible for handling all aspects of cardholder data processing. This configuration is capable of swiped or manually entered credit and swiped debit transactions.

2. OS based POS systems using the Datacap NETePay™ with dsiPDCX™ OOS with a PCI PTS compliant device with MSR. In this deployment scenario, the NETePay™ with dsiPDCX™ OOS is responsible for handling all aspects of cardholder data processing. This configuration is also capable of swiped or manually entered credit and swiped debit transactions.

Deployment Scenario 1 – Datacap NETePay™ with dsiPDCX™ OOS with Datacap PDC™ with integrated MSR and a PCI PTS compliant device

In this deployment scenario, the POS is integrated with the Datacap dsiPDCX™ OOS and a Datacap PDC™ device that has a built in MSR and an additional PCI PTS compliant device which is attached to the Datacap PDC™ device for payment card data entry and securely communicates with NETePay™ which then communicates directly with the payment processor(s). The dsiPDCX™ OOS and NETePay™ handle all aspects of authorization and settlement of the payment transaction with the payment processor(s). The POS communicates programmatically with dsiPDCX™ via formatted commands in XML that include simple transaction details such as date, time, amount, invoice number. The dsiPDCX™ OOS directly controls the MSR in the PDC™ via an RS232 connection and communicates securely to NETePay™ via TCP/IP and never returns any cardholder data to the integrated POS application. As a result, the POS system is kept out of scope of PA-DSS compliance requirements since it does not capture, store, process or transmit cardholder data as part of authorization and settlement.

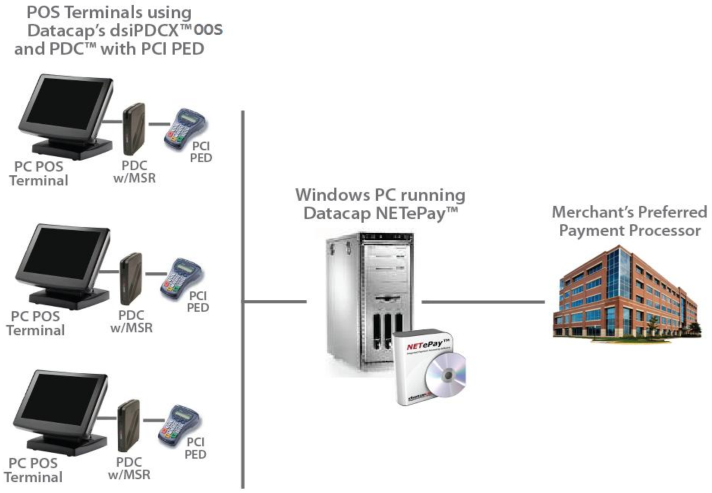


Figure 1: POS system using the **NETePay™ with dsiPDCX™ OOS** with a Datacap PDC™ with integrated MSR and a PCI PTS compliant device.

Deployment Scenario 2 – Datacap NETePay™ with dsiPDCX™ OOS and PCI PTS compliant device with MSR

In this deployment scenario, the POS is integrated with the Datacap dsiPDCX™ OOS with a PCI PTS compliant device that has an integrated MSR which is attached directly to the POS. The dsiPDCX™ control is responsible for taking payment card data directly from the PCI PTS compliant device and securely communicates with NETePay™ which then communicates directly with the payment processor(s). The dsiPDCX™ OOS and NETePay ™ handle all aspects of authorization and settlement of the payment transaction with the payment processor(s). As with the first configuration, the POS communicates programmatically with dsiPDCX™ via formatted commands in XML that include simple transaction details such as date, time, amount, invoice number. The dsiPDCX™ OOS directly controls the MSR and keypad in the attached PCI PTS device via an RS232 connection and communicates securely to NETePay™ via TCP/IP and never returns any cardholder data to the integrated POS application. As a result, the POS is kept out of scope of PA-DSS compliance requirements since it does not capture, store, process or transmit cardholder data as part of authorization and settlement.

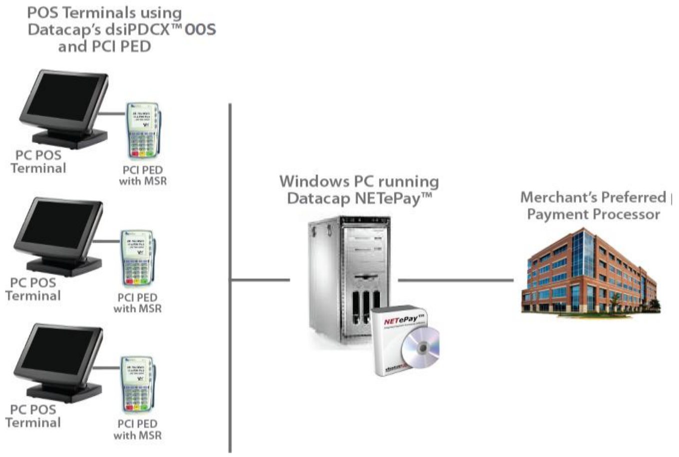


Figure 2: POS system using the **NETePay™ with dsiPDCX™OOS** and a PCI PTS compliant device with MSR.

Audience

This assessment white paper has three target audiences:

1. The first target audience includes merchants and service providers evaluating the Datacap NETePay™ with dsiPDCX™ OOS solution for deployment in their payment card environment;

2. The second target audience is partners and developers that are developing POS solutions that integrate with the Datacap NETePay™ with dsiPDCX™ OOS solution in merchant and service provider payment card environments;

3. The third target audience is the QSA and Internal Audit community that is evaluating the Datacap NETePay™ with dsiPDCX™ OOS solution or the impact of keeping the POS out of scope of PCI PA-DSS compliance in general on behalf of their merchant or service provider clients.

Assessment Scope

The scope of our assessment focused on the critical elements that validate the security and effectiveness of the "Out of Scope" (OOS) solution. In addition, we incorporated in-depth analysis of compliance fundamentals that are essential for evaluation by merchants, service providers and the QSA community.

Methodology

Coalfire has implemented industry best practices in our assessment and testing methodologies. Standard audit methods were used throughout the assessment. Coalfire conducted technical lab testing in our lab which included installation of the Datacap NETePay™ with dsiPDCX™ OOS, examination of the API integration and communication, transactional testing, device assessment, and forensic analysis.

Merchant PCI Compliance Scope

There will always be certain controls for PCI DSS compliance that must be independently assessed in any merchant's environment. PCI DSS compliance will always apply to a merchant if they transmit, process, or store credit card data anywhere in their physical environment. However, if the Datacap NETePay™ with dsiPDCX™ OOS solution is properly integrated during the development of the Point of Sale application then the POS application can remain out of scope of PCI PA-DSS validation requirements.

Technical Security Assessment

The modular design of the Datacap NETePay™ with dsiPDCX™ OOS presented Coalfire with two core deployment scenarios. Our assessment covered each core deployment architecture and included configuration options. The existing Datacap NETePay™ payment application was reviewed via the Report on Validation (ROV) completed by Coalfire in 2010.

The assessment included a comprehensive set of administration, technical, and physical control testing performed for each deployment architecture. Applicable compliance control requirement adherence from the PCI PA-DSS was validated within the scope of our security assessment. The assessment included the following components:

- Datacap NETePay™ with dsiPDCX™ OOS solution
- Datacap PDC™ (Peripheral Device Controller) device with MSR
- PCI PTS compliant Device (VFI Vx810 with MSR)
- POS emulation on a Windows 7 platform with dsiPDCX™
- XML Command Sets (dsiPDCX™ was used to issue commands)

Summary Findings

The following findings are relevant highlights from this assessment.

- The NETePay™ with dsiPDCX™ OOS solution integrates securely with POS systems without exposing card data to these platforms.
- Simple transactional data is only required for payment transactions including date, time, dollar amount, and invoice number.
- The NETePay™ with dsiPDCX™ OOS or PCI Compliant PTS device must be the only point that captures card data through swiped or keyed entry in order to achieve the desired PA-DSS scope elimination of the POS.
- A payment application or POS that is not PABP/PA-DSS validated can be taken out of PCI scope if all payment data is captured through the NETePay™ with dsiPDCX™ OOS solution (for POS systems where the application vendor has introduced this capability through an upgrade, the systems must be cleansed of all legacy card data.)
- A NETePay™ with dsiPDCX™ OOS solution will not remove PCI control requirements for network firewall, network configuration, physical controls and administrative procedures for a merchant.

Assessor Comments

Our assessment scope put a significant focus on validating the removal of PCI PA-DSS scope when integrating any POS payment application with Datacap's NETePay™ with dsiPDCX™ OOS solution. The Datacap NETePay™ with dsiPDCX™ OOS solution can benefit POS developers by removing the cost of a PCI PA-DSS compliance assessment and validation, thus providing an increased value proposition to their clients.

It is also important to note that an 'Out of Scope' solution, as detailed in this whitepaper, does not alleviate a merchant's responsibility to PCI DSS compliance requirements. Security and business risk mitigation should always be a merchant's goal and focus for selecting security controls such as this OOS solution.

PCI PA-DSS Compliance

Applicability of PA-DSS

The PCI PA-DSS applies to a payment application (as defined by PCI SSC) as follows: "The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties (PCI PA-DSS Version 2.0, 2010, October: Page 5)."

Coalfire's Assessment

Datacap's NETePay™ with dsiPDCX™ OOS solution provides a complete solution to capture, process, transmit and/or store cardholder data as part of authorization or settlement. As a result, Point of Sale (POS) applications which integrate to Datacap's NETePay™ with dsiPDCX™ OOS solution as the only point of capture, storage, processing or transmittal of cardholder data may be removed from scope of PA-DSS compliance requirements as they are no longer "payment aware" and don't fit in the defined PA-DSS program of PCI SSC.

Coalfire Assessment Information

Assessment Environment

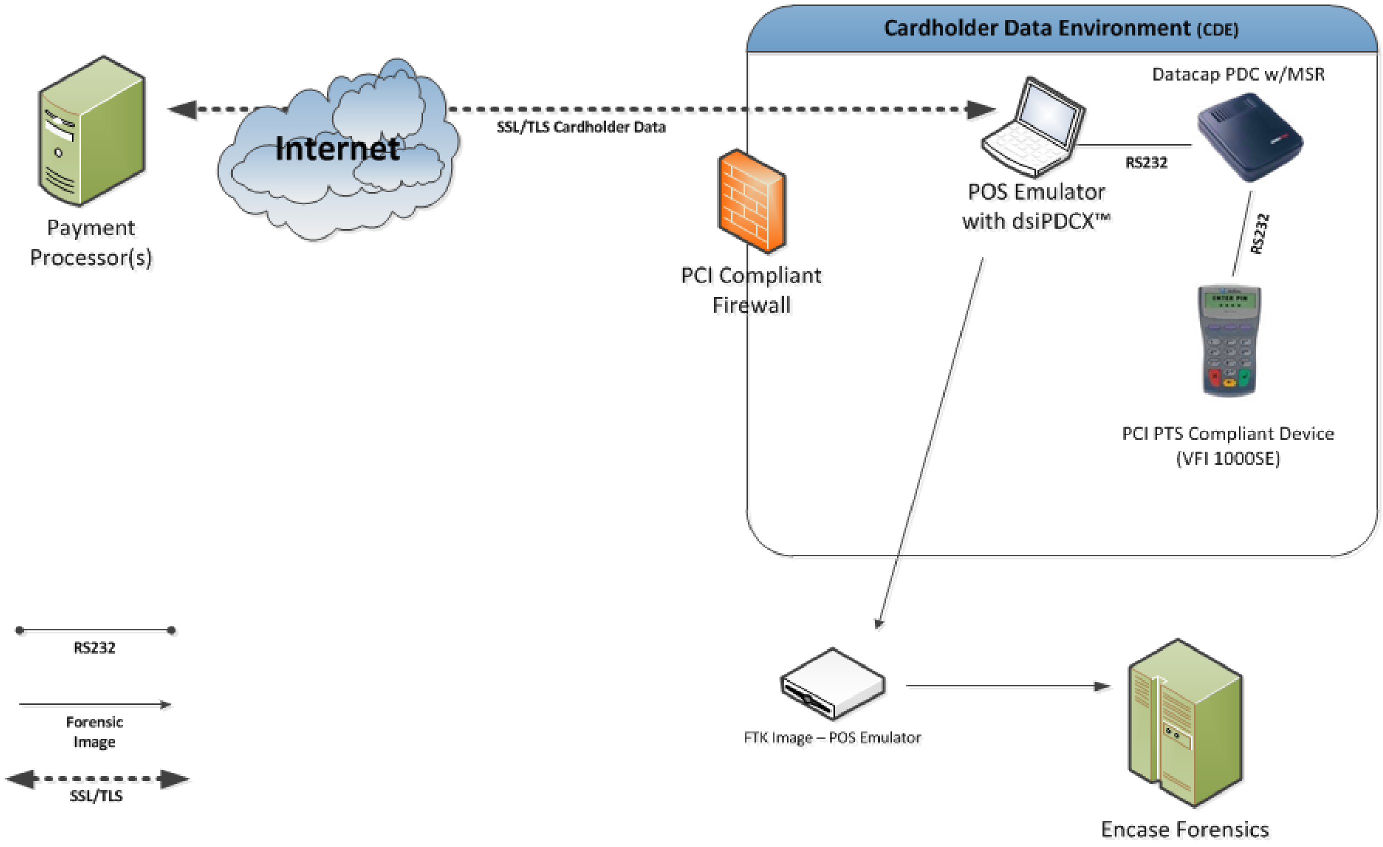
Datacap NETePay™ with dsiPDCX™ OOS was installed in Coalfire's Lab for the duration of the testing. The assessment included a lab system running a POS Emulator connected with the appropriate hardware for the tested configuration. The assessment also included transactional testing; monitoring interfaces for transmitted data and scanning the disk for any cardholder and sensitive authentication data.

The test equipment and software consisted of:

1. Wireshark Ethernet port sniffer to monitor traffic between the Datacap dsiPDCX™ and NETePay™.
2. Encase was used to perform forensics analysis.

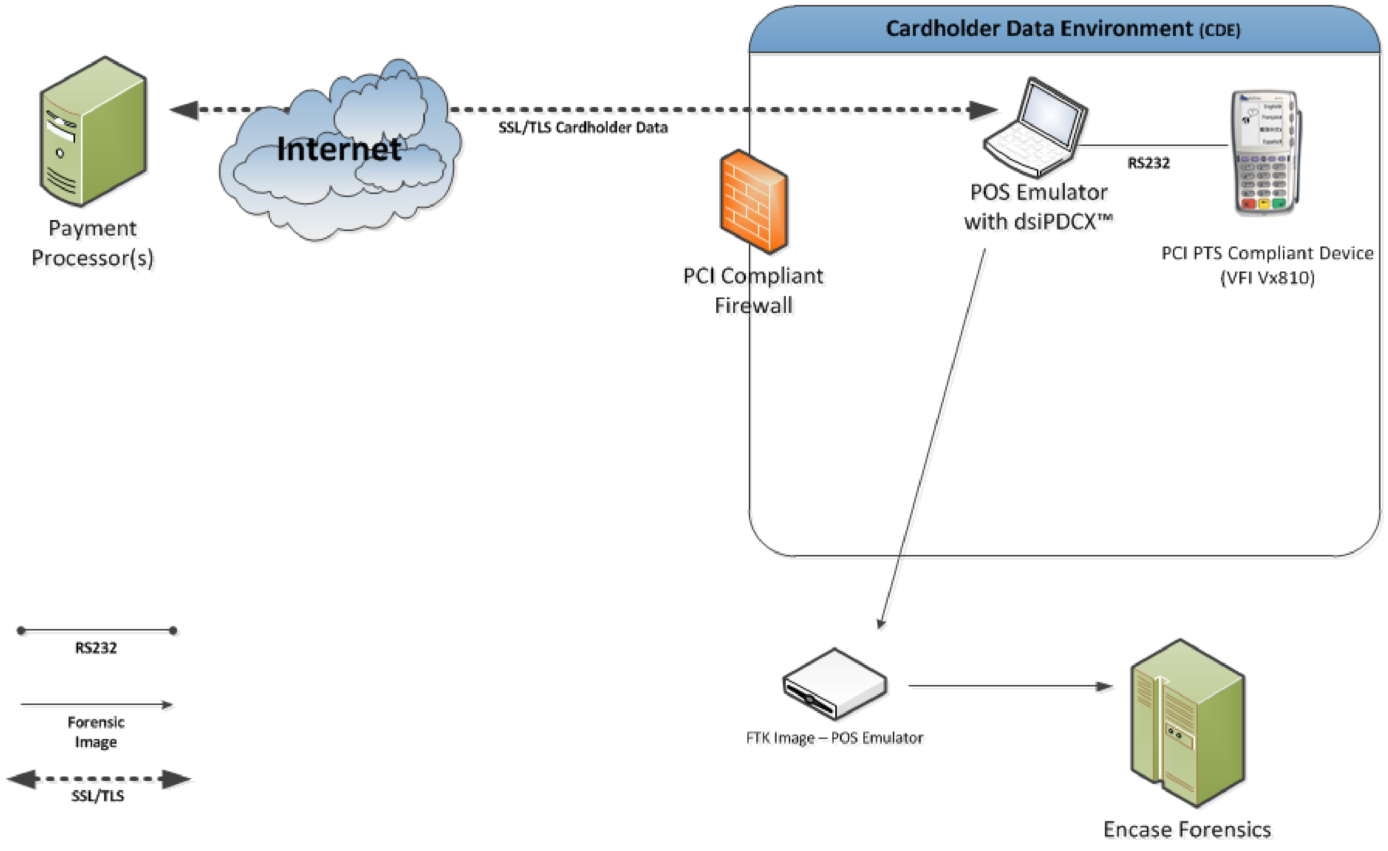
Test Lab Configuration Diagram 1 – Datacap NETePay™ with dsiPDCX™ OOS with Datacap PDC™ with integrated MSR and a PCI PTS compliant device

The diagram below illustrates configuration used to test *the Datacap NETePay™ with dsiPDCX™* OOS solution in scenario 1. A Datacap PDC™ and a VFI 1000SE were utilized for testing.



Datacap NETePay™ with dsiPDCX™ OOS and PCI PTS compliant device with MSR

The diagram below illustrates configuration used to test *the Datacap NETePay™ with dsiPDCX™* OOS solution in scenario 2. A VFI Vx810 was utilized for testing.



Disk Analysis

The technical assessment included a forensic examination of the hard drive of the system running the TranManagement software which also had the Datacap TRAN OOS devices connected.

The process for examining the hard drives was as follows:

1. FTK was utilized to create a forensic image of the system hard drive with the POS emulator and attached Datacap NETePay™ with dsiPDCX™ OOS solution devices.

2. EnCase was used to search the disk image for key criteria, including cardholder and sensitive authentication data.

No findings were identified. The following represents the conclusions from performing forensic analysis:

1. The disk forensic analysis demonstrates that there is no residual cardholder or sensitive authentication data on the system running the POS emulator.

Network Traffic Assessment

A Wireshark Ethernet port sniffer was used to monitor traffic from the POS emulator system running the dsiPDCX™ interface and attached hardware to the payment processor. The captures indicate no unencrypted data is being transmitted over the network and that no communication of cardholder data or sensitive authentication data to the POS destination IP address occurred.

Tools and Techniques

Standard tools Coalfire utilizes for its application security reviews can include:

Tool Name	**Description**
Encase	*Forensic tool for digital data & media analysis.
Additional tools	Various Search Engines, Whois and DNS Enumeration, Usenet, Google Hacking Database, Wikto, Wayback Machine, Sam Spade, Cain&Able, NMAP Nessus, Netcat, Dsniff, Wireshark, THC Hydra, THC SSLCheck, SslScan, Nikto, MiB Browser, soapUI, NIST CVSS 1998-2009 Archive List., Rapid 7 Community

*Forensic tool: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly.