# TwinTran

## PA-DSS 2.0 Dealer Guide

Version 3.80

8 October 2013


Datacap Systems Inc.

Leon Morsillo

Vice President, Engineering


**Table of Contents**

# Notice

**THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Datacap Systems Inc. MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER Datacap Systems Inc. NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.**

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

**The retailer may undertake activities that may affect compliance. For this reason, Datacap Systems Inc. is required to be specific to only the standard software provided by it.**

# About this Document

This document describes the steps that must be followed in order for your TwinTran installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 2.0 dated October, 2010).

Datacap Systems Inc. instructs and advises its customers to deploy Datacap Systems Inc. applications in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various "Benchmarks", should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

**You must follow the steps outlined in this *Implementation Guide* in order for your TwinTran installation to support your PCI DSS compliance efforts.**

# Revision Information

| Name | Title | Date of Update | Summary of Changes |
|---|---|---|---|
| TwinTran | Tran Series 3.0 Implementation Guide | 27 Sept 2010 | Initial Release for PCI Security Standards Council Payment Application Data Security Standards program (version 1.2 dated October, 2008). |
| TwinTran | Tran Series 3.0 Implementation Guide | 03 Oct 2011 | Annual Review. No content changes. |
| TwinTran | Tran Series 3.0 Implementation Guide | 01 Oct 2012 | Annual Review. No content changes. |
| TwinTran | TwinTran PA-DSS 2.0 Implementation Guide | 08 Oct 2013 | Update for PA-DSS V2.0. Tran models segmented into individual model Implementation Guides. |
| | | | |

This PA-DSS Implementation Guide will be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates will be tracked and reasonable accommodations will be made to distribute or make the updated guide available to users. Datacap Systems Inc. will distribute the IG to new customers via web download.

# Executive Summary

TwinTran version 3.80 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):


| | |
|---|---|
| Coalfire Systems, Inc.<br>361 Centennial Parkway Suite 150<br>Louisville, CO 80027 | Coalfire Systems, Inc.<br>150 Nickerson Street Suite 106<br>Seattle, WA 98109 |

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP)
  http://www.owasp.org

# Application Summary

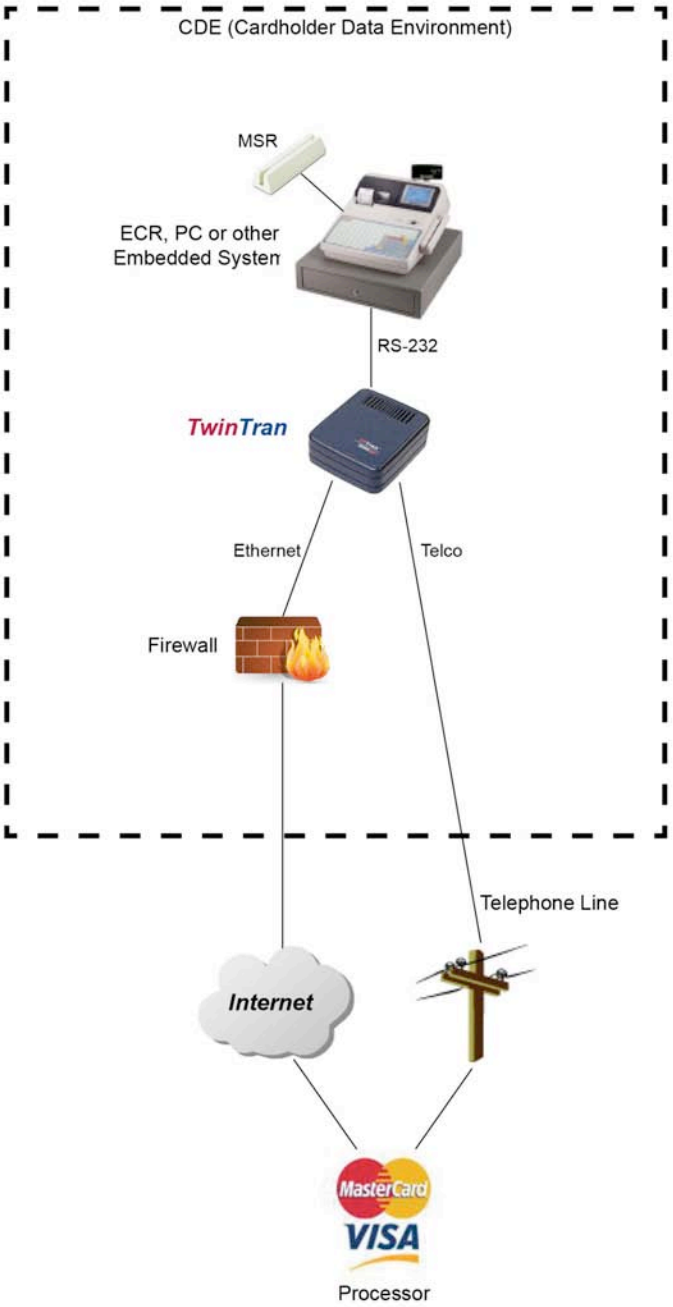
| | |
|---|---|
| **Payment Application Name:** | TwinTran |
| **Payment Application Version:** | 3.80 |
| **Application Description:** | TwinTran is a self-contained proprietary hardware device designed to load and execute applications solely developed by Datacap Systems Inc. for the purpose of processing credit/debit payment transactions. TwinTran communicates with a payment processor via the Internet or dial-up modem connection as a back up.<br><br>The TwinTran device interfaces with the 3rd party OEM payment applications/devices via a dedicated RS232 serial connection. Datacap provides OEM payment application vendors with a |

<table>
<tr><td></td><td>specification of the commands required to interface with the TwinTran device.<br><br>The TwinTran device can be loaded by Datacap with applications which are payment processor specific, e.g. TSYS, Paymentech, Fifth Third, etc. The TwinTran device employs the communications standards required by each processing provider; no end-user configuration of processor communications parameters is possible.</td></tr>
<tr><td>Application Target Clientele:</td><td>The target clientele is 3rd party developers of POS/ECR systems. The TwinTran device is primarily used in Retail; Restaurants; Mail Order/Telephone Order services; and E-Commerce.</td></tr>
<tr><td>Components of Application Suite (i.e. POS, Back Office, etc.)</td><td>TwinTran Application Device</td></tr>
<tr><td>Required Third Party Payment Application Software:</td><td>None<br><br>No third party payment software is required. All code hosted on the TwinTran device is developed and maintained by Datacap.</td></tr>
<tr><td>Database Software Supported:</td><td>None</td></tr>
<tr><td>Other Required Third Party Software:</td><td>None</td></tr>
<tr><td>Operating System(s) Supported:</td><td>Windows CE.NET 4.2 (Core)</td></tr>
<tr><td>Application Functionality Supported</td><td>Select one or more from the following list:
<table>
<tr><td>☐</td><td>POS Suite</td><td>☐</td><td>POS Admin</td><td>☐</td><td>Shopping Cart & Store Front</td></tr>
<tr><td>☐</td><td>POS Face-To-Face</td><td>☒</td><td>Payment Middleware</td><td>☐</td><td rowspan="3">Others (Please Specify):</td></tr>
<tr><td>☐</td><td>POS Kiosk</td><td>☐</td><td colspan="2">Payment Back Office</td></tr>
<tr><td>☐</td><td>POS Specialized</td><td>☐</td><td colspan="2">Payment Gateway/Switch</td></tr>
</table></td></tr>
<tr><td>Payment Processing Connections:</td><td>The TwinTran device interfaces with the 3rd party OEM payment applications/devices via an RS232 serial connection.<br><br>The OEM payment application captures the card data and passes the sensitive authentication or cardholder data to the TwinTran in a transaction request message over the dedicated RS-232 connection. The TwinTran reformats and encrypts an authorization message and sends it to the payment processor using a secure protocol over an IP network or via a dial-up modem connection when IP is not available. When the TwinTran receives a response from the payment processor, it decrypts and formats a response message, which it sends to the OEM payment application over the RS-232 interface.<br><br>The TwinTran device never stores sensitive authentication data. The TwinTran device uses flash memory to store settlement data. Settlement data is encrypted cardholder data (i.e. PAN) and does</td></tr>
</table>

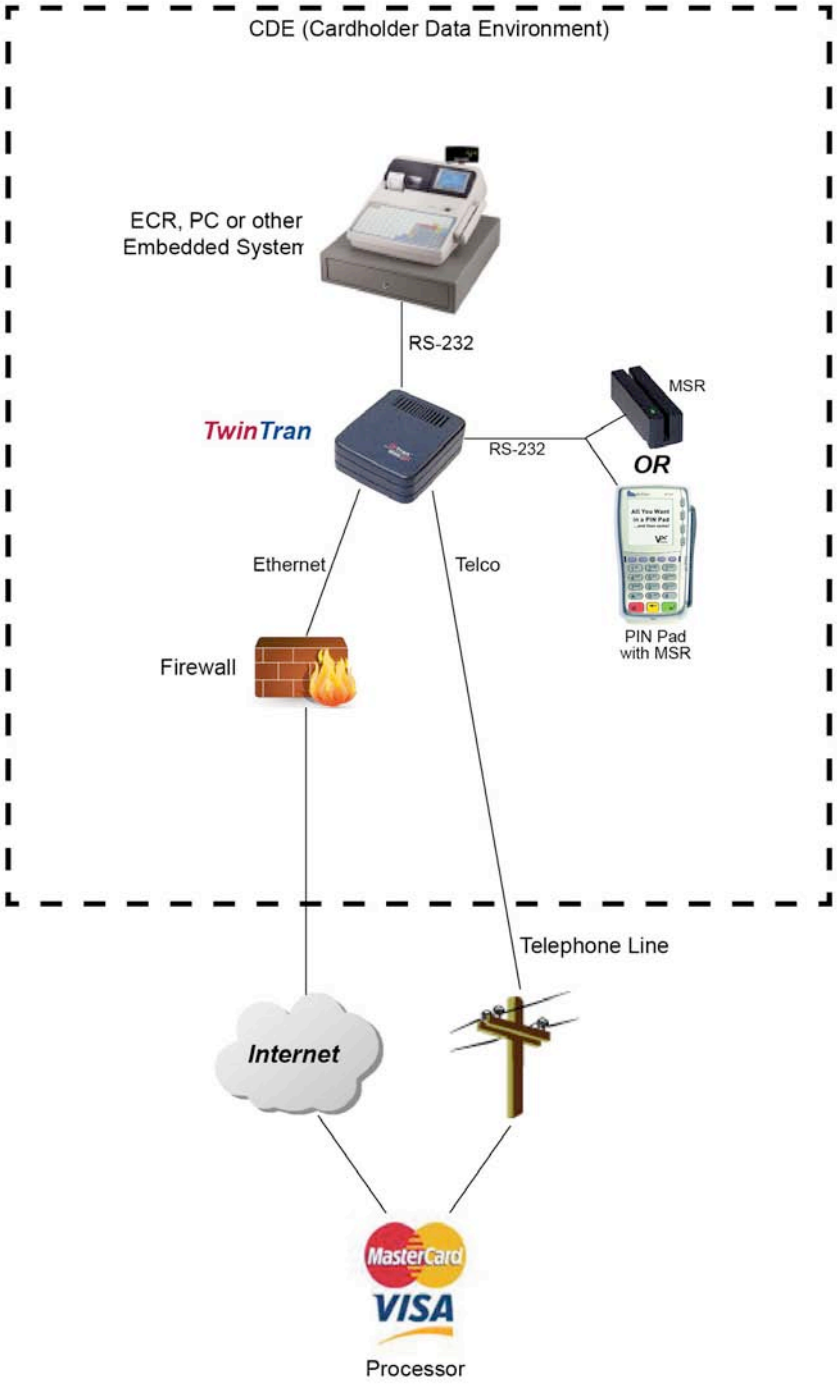
| | |
|---|---|
| | not include sensitive authentication data. Once settlement takes place, the settlement data is securely purged from the TwinTran flash memory. |
| **Application Authentication** | TwinTran does not support any remote or console access or insecure network connections.<br>TwinTran communicates with Payment Processing Providers using either secure protocols (SSL/TLS/HTTPS) via IP/Internet (or a dial-up modem connection when IP/Internet is not available) that are specified by the Payment Processing Provider. TwinTran does not support any Processing Provider that uses an insecure IP protocol. TwinTran presents user credentials (in the form of Payment Processing Provider assigned Merchant ID and Terminal ID) in every message containing cardholder data to the Payment Processing Provider. The Payment Processing Provider validates the Merchant ID and Terminal ID values as a prerequisite for host access and processing. |
| **Description of Versioning Methodology:** | DialTran payment applications are assigned versions for internal source code management and release control as follows:<br>X.Y.Z<br>Where:<br>X = represents significant functional changes and/or to reflect assessment with major PA-DSS standard update.<br>Y = represents significant functional changes or to correct minor PA-DSS security issues.<br>Z = Functional enhancements or maintenance updates unrelated to PA-DSS compliance issues. This number designation is not a part of the PA-DSS version number and is tracked internally at Datacap. |
| **List of Resellers/Integrators (If Applicable)** | Datacap Systems Inc. considers its integrator and reseller information as confidential and proprietary. Contact Datacap Systems Inc. for additional information on the dealer program. |

## Typical Network Implementations

### *1. TwinTran – In Scope Component Diagram*

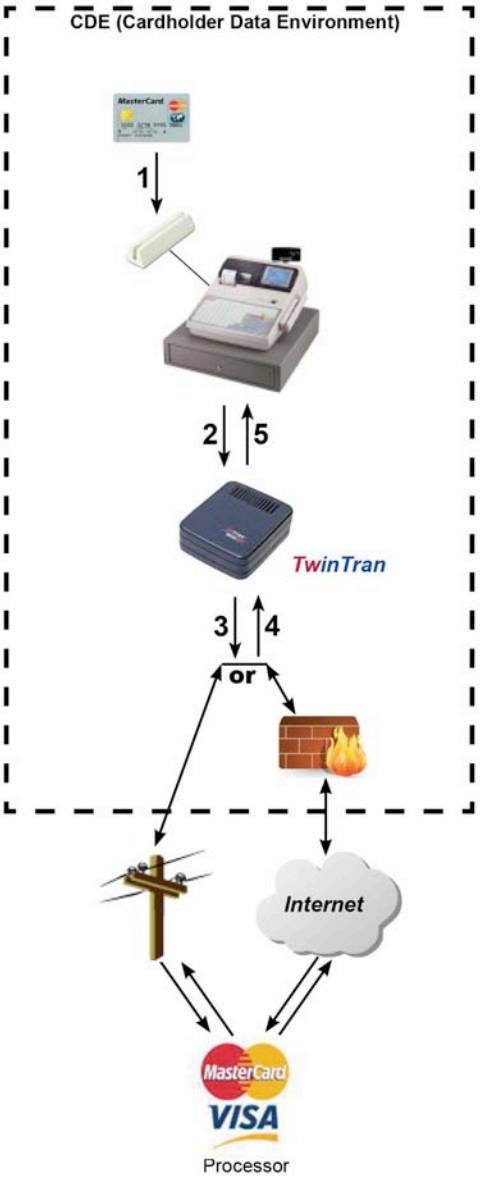


## 2. *TwinTran – Out of Scope Component Diagram*



# TwinTran Data Flow and Data Handling Diagrams

## *1. TwinTran – In Scope Data Flow and Data Handling Diagram*




**Authorization Flow**

1. A card is swiped on an MSR (magnetic stripe reader capable of reading ABA format data on track 2) connected to ECR, PC or embedded (host) device. If a card is unreadable in the MSR, then the account number and expiration date are entered via a keyboard on the host device by an operator.

2. The host device creates a Tran authorization command which includes the stripe data or hand keyed account number and expiration date and transmits the command over the command interface connection to the TwinTran.

3. The TwinTran reformats the received authorization command into a message that the processor will be able to process. The TwinTran encrypts/formats the message according to the processor's requirements and transmits it using IP over the network (Internet or dedicated connection) or dial-up modem connection to the processor.

4. The processor transmits its encrypted (IP) or proprietary (dial-up) response back to the TwinTran.

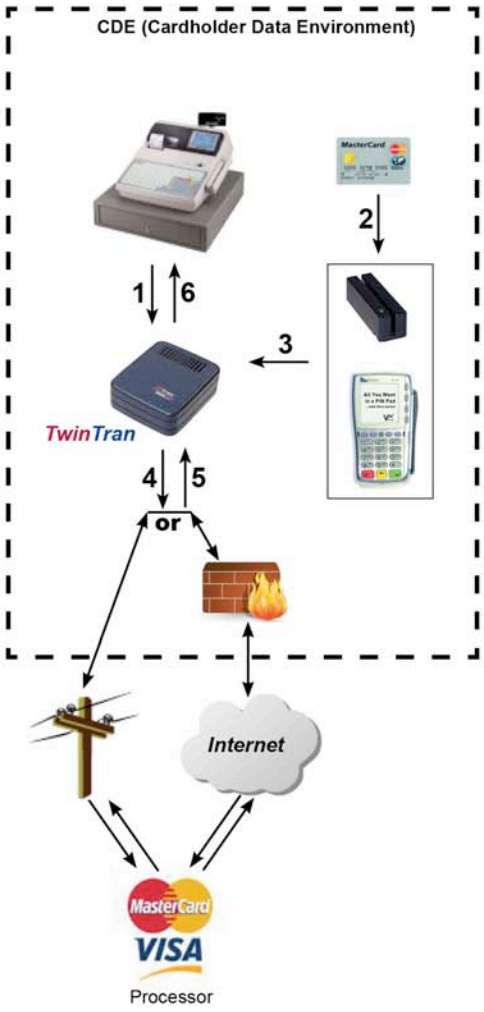
5. The TwinTran decrypts/decodes the processor response and reformats it into an TwinTran response message and transmits it back to the host device over the command interface connection.

**Settlement Flow**

At the conclusion of the processing cycle (typically daily) the host device will issue a batch close (settlement) command (2) to the TwinTran. If the TwinTran is loaded with software for a terminal-based processing network, it will transmit the collected transaction records using IP (3) over the network (Internet or dedicated connection) or dial-up modem connection to the processor. If the TwinTran is loaded with software for a host-based processing network, the TwinTran does not transmit the collected transaction records to the processor but sends a settlement request. The processor replies with the result of the settlement action to the TwinTran (4) and the TwinTran reports the results to the POS/ECR (5). In either case, upon completion of settlement, the TwinTran closes the batch and marks all collected transaction records to be securely deleted automatically upon the next batch open command from the host device. Once a batch close is completed, the TwinTran is not able to process additional transactions until it receives a batch open command.

If the host device (ECR/POS) issues a batch clear command, the TwinTran will unconditionally, immediately and securely delete any stored batch information.

## 2. *TwinTran – Out of Scope Data Flow and Data Handling Diagram*




**Authorization Flow**

1. The host device creates a Tran authorization command over the command interface connection to the TwinTran.
2. A card is swiped on an MSR or PIN Pad with MSR (magnetic stripe reader capable of reading ABA format data on track 2) connected to TwinTran. If a card is unreadable and a PIN Pad with MSR is employed, then the account number and expiration date are entered via the PIN Pad keyboard by the cardholder. No cardholder information is transmitted to the host device.
3. The TwinTran receives the MSR or keyed account information and creates an authorization message according to the requirements of the processor.
4. The TwinTran encrypts/formats the message according to the processor's requirements and transmits it using IP over the network (Internet or dedicated connection) or dial-up modem connection to the processor.
5. The processor transmits its encrypted (IP) or proprietary (dial-up) response back to the TwinTran.
6. The TwinTran decrypts/decodes the processor response and reformats it into an TwinTran response message and transmits it back to the host device over the command interface connection. No cardholder information is transmitted to the host device.

**Settlement Flow**

At the conclusion of the processing cycle (typically daily) the host device will issue a batch close (settlement) command (1) to the TwinTran. If the TwinTran is loaded with software for a terminal-based processing network, it will transmit the collected transaction records using IP (4) over the network (Internet or dedicated connection) or dial-up modem connection to the processor. If the TwinTran is loaded with software for a host-based processing network, the TwinTran does not transmit the collected transaction records to the processor but sends a settlement request. The processor replies with the result of the settlement action to the TwinTran (5) and the TwinTran reports the results to the POS/ECR (6). In either case, upon completion of settlement, the TwinTran closes the batch and marks all collected transaction records to be securely deleted automatically upon the next batch open command from the host device. Once a batch close is completed, the TwinTran is not able to process additional transactions until it receives a batch open command. No cardholder information is transmitted to the host device at any point in the settlement process.

If the host device (ECR/POS) issues a batch clear command, the TwinTran will unconditionally, immediately and securely delete any stored batch information.

**Out of Scope TwinTran configurations** provide a complete solution to capture, process, transmit and/or store cardholder data as part of authorization or settlement. As a result, host devices (ECR/POS), which integrate to TwinTran's out of scope configuration, *may* be removed from scope of PA-DSS compliance requirements, as they may be no longer payment aware. Consult your Qualified Security Assessor (QSA) and/or Payment Application Qualified Security Assessor (PA- QSA) for qualification opinion of systems using this configuration.

## Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be "PA-DSS Validated."

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining "PCI Compliance" is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

### *The 12 Requirements of the PCI DSS:*

***Build and Maintain a Secure Network***

1. *Install and maintain a firewall configuration to protect data*
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*

***Protect Cardholder Data***

3. *Protect Stored Data*
4. *Encrypt transmission of cardholder data and sensitive information across public networks*

***Maintain a Vulnerability Management Program***

5. *Use and regularly update anti-virus software*
6. *Develop and maintain secure systems and applications*

***Implement Strong Access Control Measures***

7. *Restrict access to 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*

## Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

- Sensitive Authentication Data requires special handling
- Remove Historical Cardholder Data
- Set up Good Access Controls
- Properly Train and Monitor Admin Personnel
- Key Management Roles & Responsibilities
- PCI-Compliant Remote Access
- Use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of administrative access
- Log settings must be compliant
- PCI-Compliant Wireless settings
- Data Transport Encryption
- PCI-Compliant Use of Email
- Network Segmentation
- Never store cardholder data on internet-accessible systems
- Use SSLV3 for Secure Data Transmission
- Delivery of Updates in a PCI Compliant Fashion

## Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a)

Previous versions of TwinTran applications did not store sensitive authentication data. Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v2.0.

## Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c)

Datacap Systems Inc. does not store Sensitive Authentication data for any reason, and we strongly recommend that you do not do this either. However, if for any reason you should do so, the following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when needed to solve a specific problem
- Store such data only in specific, known locations with limited access

- Collect only the limited amount of data needed to solve a specific problem
- Encrypt sensitive authentication data while stored
- Securely delete such data immediately after use

## Purging of Cardholder Data (PA-DSS 2.1)

The following guidelines must be followed when dealing with cardholder data (PAN alone or with any of the following: expiry date, cardholder name or service code):

- A customer defined retention period must be defined with a business justification.
- Cardholder data exceeding the customer-defined retention period must be purged.
- To purge the cardholder data in TwinTran you must do the following:

TwinTran applications store unsettled transactions containing cardholder data in an *encrypted* batch in flash memory that is permanently soldered to the logic board and is not removable. All transactions (and associated cardholder data) are automatically, permanently and securely purged when a batch is settled, cleared or an application is loaded or reloaded. Batches are of fixed maximum size (which vary by payment processor) and when a batch is filled, no further transactions may be performed until the existing batch is settled or cleared.

A user may manually initiate the purge of all TwinTran transactions (and associated cardholder data) by performing a batch settle or clear command.

Any cardholder data you store outside of the TwinTran application must be documented and you must define a retention period at which time you will purge (render irretrievable) the stored cardholder data.

## Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a)

TwinTran applications incorporate an automatic key generation methodology that creates a unique dynamic key for each batch. This function cannot be disabled or configured by a user and requires no user key management or custodial functions.

## Removal of Cryptographic material (PA-DSS 2.7.a)

Previous versions of TwinTran never stored historic cardholder data; only unsettled transaction information is stored in TwinTran. Once transaction items (and associated cardholder data) in TwinTran storage are settled or cleared, they are securely and permanently deleted.

TwinTran applications automatically create a unique dynamic key for each batch. Upon settlement, batch or application load or reload, a new unique dynamic key is automatically created and used for batch encryption.

## Set up Strong Access Controls (3.1.a and 3.2)

TwinTran is a proprietary design hardware device that employs a microcontroller running fixed, flash loaded software created and controlled solely by Datacap Systems Inc. As a hardware device, TwinTran hardware is physically and functionally self-contained and users are unable to alter or inspect software or data directly.

TwinTran devices are designed to be attached via a dedicated continuous RS232 connection to a host device (ECR/POS) that will utilize its payment processing functions. Host devices (ECR/POS) that communicate with TwinTran must employ a command syntax structure defined by Datacap. Any communications that do not strictly conform to the defined command structure will be ignored by the TwinTran application.

TwinTran commands are limited to payment processing functions only; no direct inspection or changes to TwinTran software or memory are implemented. TwinTran applications do not support any administrative or inquiry commands that return complete cardholder data (i.e. account numbers and expiration dates). Once cardholder data is stored in a batch, it may not be retrieved in any form that includes complete cardholder data (i.e. account numbers and expiration dates).

Datacap advises developers and manufacturers of host devices (ECR/POS) that use TwinTran that the PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords according to PA-DSS V2.0 sections 3.1.a and 3.2.

## Properly Train and Monitor Admin Personnel

It is your responsibility to institute proper personnel management techniques for allowing admin user access to cardholder data, site data, etc. You can control whether each individual admin user can see credit card PAN (or only last 4).

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust into your admin site and whom you allow to view full decrypted and unmasked payment information.

## Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)

Since TwinTran is physically and functionally independent of a connected system or service that uses its capabilities, it does not record historical logs of command processing activity beyond that for transactions that have not yet been settled.

Typical TwinTran configurations include ECR's (Electronic Cash Registers) that are usually proprietary self-contained devices that have keyboard, display, printer, RS232 and memory storage. A typical ECR will usually include electronic journal capability that allows an operator to view TwinTran activity over time with time stamping, function and operator information included.

In addition, most payment processing service providers (e.g. TSYS, Paymentech, GPS, Fifth Third, etc.) supported by TwinTran have web portals which allow a merchant secure access to view recent and historical transaction activity generated by TwinTran for their account.

## Services and Protocols (PA-DSS 5.4.c)

TwinTran does not require nor permit the use of any insecure services or protocols. Here are the services and protocols that TwinTran does require:

SSL 3.0
TLS 1.0

TwinTran incorporates an internal dial-up modem that is used as a backup communications method if the primary IP/Internet communications is unavailable. TwinTran uses the dial-up messages and protocols specified by the individual payment processing provider for modem communications.

## PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b)

TwinTran does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 1.2.3, 2.1.1 and 4.1.1:

2.1.1: Change wireless vendor defaults per the following 5 points:

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions Refer to wireless device manufacturer's documentation for change instructions.
2. Default SNMP community strings on wireless devices must be changed. Refer to wireless device manufacturer's documentation for change instructions.
3. Default passwords/passphrases on access points must be changed. Refer to wireless device manufacturer's documentation for change instructions.
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. Refer to wireless device manufacturer's documentation for firmware update instructions. Firmware updates should be performed for any wireless networking device that is capable, including routers, access points, gateways and switches.
5. Other security-related wireless vendor defaults, if applicable, must be changed. Refer to wireless device manufacturer's documentation for change instructions. Changes to vendor defaults settings should be performed for any wireless networking device that is capable, including routers, access points, gateways and switches.

1.2.3: Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.
Note: The use of WEP as a security control was prohibited as of June 30, 2010.

## Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b)

Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.)

## PCI-Compliant Remote Access (10.2)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase
2. Something you have, such as a token device or smart card
3. Something you are, such as a biometric

## PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

TwinTran does not allow, nor respond to, unsolicited incoming traffic on the Ethernet/IP port nor does it answer any incoming calls via the internal modem. On-demand remote initiated access functions are not supported. Datacap Systems Inc. does not deliver separate patches and updates for TwinTran. All TwinTran application updates needed to address security issues are released as a full installation of new TwinTran software.

As a development company, we keep abreast of the relevant security concerns and vulnerabilities in our area of development and expertise.

Our continuing security education activities are comprised of the following:

- Participating in Microsoft E-Learning Security Clinics and Hands-On Labs
- Attendance of live Microsoft security seminars
- Encourage recommendations for technical library purchases on security subjects
- Regular review of OWASP (Open Web Application Security Project) website (http://www.owasp.org)
- Regular review of US-CERT (United States Computer Emergency Readiness Team) Current Activity (http://www.us-cert.gov/current/)
- Regular review of SecurityTracker 's Weekly Vulnerability Summary Newsletter distributed via email

Once we identify a relevant vulnerability, we work to develop and test an updated TwinTran application that helps protect TwinTran against the specific, new vulnerability. We attempt to publish an updated application within 10 days of the identification of the vulnerability. We will then contact vendors and dealers to encourage them to install the updated application. Typically, merchants are expected to respond quickly to and install available updated applications within 30 days.

We do not deliver software and/or updates via remote access to customer networks. TwinTran application software and configurations are loadable only by Datacap's PSCS (Payment Systems Configuration Server) web accessible system; Internet connectivity is required for PSCS communications, dial-up access to PSCS is not supported. Datacap maintains sole ability and responsibility for access for posting TwinTran software and updates to the PSCS web service.

A user may establish a PSCS account with Datacap (requiring a username and password) and select a TwinTran payment service module (application) created by Datacap to communicate with the payment service provider of their choice. The PSCS user must establish a relationship in PSCS between the selected application and configuration data and the TwinTran DID for loading of TwinTran to occur.

TwinTran always initiates communications with the PSCS system; PSCS cannot initiate program or configuration loads to TwinTran. The PSCS system keeps complete logs of user and Tran loading activity. PSCS applications and configuration data do not contain any cardholder information. TwinTran may have only one processor specific application loaded at any time; reloads by PSCS replace the existing application load with new application software. The PSCS web server employs a singed certificate and SSL to deliver TwinTran applications and configurations.

## PCI-Compliant Remote Access (10.3.2.b)

TwinTran does not support any remote access functionality.

If users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for PCAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions:

- Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses

- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

## Data Transport Encryption (PA-DSS 11.1.b)

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128 bit encryption strength (either at the transport layer with SSLV3 or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSLV3) / transport layer security (TLS 1.0 or higher) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- The Internet
- Wireless technologies
- Global System for Mobile Communications (GSM)
- General Packet Radio Service (GPRS)

TwinTran uses SSL 3.0 or TLS 1.0 (or higher) encryption for all IP communications; for dial-up modem connections, it uses the messages and protocols specified by the payment processing provider. Refer to the Dataflow diagrams for an understanding of the flow of encrypted data associated with TwinTran.

## PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b)

TwinTran does not allow or facilitate the sending of PANs via any end user messaging technology (for example, e-mail, instant messaging, and chat).

## Non-console administration (PA-DSS 12.1)

Although TwinTran does not support non-console administration and we do not recommend using non-console administration, should you ever choose to do this, must use SSH, VPN, or SSLV3/TLS 1.0 or higher for encryption of this non-console administrative access.

## Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for Internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming Internet traffic to the trusted application environment can be allowed. Additionally, outbound Internet access from the trusted segment must be limited to required and justified ports and services.

- Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with TwinTran.

# Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
- Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for on-going compliance and assessment.
- Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts as needed.

# Application System Configuration

TwinTran is a proprietary design hardware device that employs a microcontroller running fixed, flash loaded software created and controlled by Datacap Systems Inc. TwinTran applications are complete load images built with Windows CE.NET 4.2 (Core) and do not support any HID devices or displays.

As a hardware device, TwinTran hardware is physically and functionally self-contained and users are unable to alter or inspect software or data directly. Since TwinTran is physically and functionally independent of a connected system or service that uses its capabilities, it does not require a specific host device system configuration beyond the capability to communicate Datacap defined commands over an RS-232 connection.

Datacap recommends that all relevant sections of the latest PCI DSS standards for proper maintenance be applied to host devices using TwinTran, where applicable.

## Payment Application Initial Setup & Configuration

**Installing the TwinTran Payment Application**

TwinTran is a proprietary design hardware device that employs a microcontroller running fixed, flash loaded software created and controlled solely by Datacap Systems Inc. As a hardware device, TwinTran hardware is physically and functionally self-contained and users are unable to alter or inspect software or data directly. TwinTran devices are designed to be attached via a dedicated continuous RS232 connection to a host device (ECR/POS) that will utilize its payment processing functions.

Before a TwinTran device can be used to process payment requests, it must be loaded with a payment service specific application (e.g. TSYS, Paymentech, GPS, Fifth Third, etc.) and user specific account configuration data. TwinTran software and configurations can be loaded by Datacap's PSCS (Payment Systems Configuration Server) web accessible system. PSCS access by TwinTran is controlled at the hardware level by a unique DID (Device ID) that is incorporated into the TwinTran hardware at manufacture and cannot be altered by a user. A user may establish a PSCS account with Datacap (requiring a username and password) and select a TwinTran payment service module (application) created and certified by Datacap to communicate with the payment service provider of their choice. The PSCS user must establish a relationship in PSCS between the selected application and configuration data and the TwinTran DID for loading of TwinTran to occur. TwinTran may have only one processor specific application loaded at any time; reloads by PSCS replace the existing application load with software.

Once a PSCS profile has been created for a particular TwinTran DID on PSCS, the TwinTran can be commanded by the host device (ECR/POS) to contact the PSCS server to retrieve and load the associated application and configuration data.

**Defining the Payment Gateway**

Each TwinTran application is designed to communicate with a specific payment processing service (e.g. TSYS, Paymentech, GPS, Fifth Third, etc.) using the protocol, message formats and encryption defined by that processor. The gateway address for each processing provider is included in the TwinTran application specific to that provider as a URI/URL and is not directly changeable by a user.

**Conducting Test Transactions**

Datacap includes printed instructions with each TwinTran device on performing test transactions prior to using it in production.

**Special Instructions for Upgrades**

Once a TwinTran device has been successfully loaded with a processor application and

configuration by Datacap's PSCS system, it will function indefinitely. If an update to address a processing provider change or security vulnerability is necessary, Datacap will inform TwinTran distributors, resellers and users according to it's SDLC process. Users will be required to make appropriate PSCS changes and initiate a load request from PSCS from the host device (ECR/POS).