# Evosus® Business Management System
# Version 6.5
# PA-DSS Implementation Guide

# Table of Contents

# Review / Revision History

| Version # | Date | Author/Reviewer | Description |
|---|---|---|---|
| Initial Draft v 1.0 | 6/02/2010 | Steve Hawkins | Initial draft |
| Release v 1.1 | 7/09/2010 | Steve Hawkins | Internal circulation |
| Release v 1.2 | 09/16/2010 | Steve Hawkins | Released for review |
| Release v 1.3 | 09/29/2011 | Steve Hawkins | Released to Halock. Add references to logging in Evosus. |
| Release v 1.4 | 10/17/2011 | Steve Hawkins | Add instructions for System Backups that do not retain sensitive cardholder data. |
| Release v 1.5 | 11/11/2016 | Steve Hawkins & David Weisong | Revisions for PA-DSS v3.2 Requirements |

This implementation guide is reviewed at least annually and updated when changes to software and/or PA-DSS requirements occur.

# 1 Payment Systems Security

## *1.1 Introduction*

In order to address the growing national and international concern for securing credit card information, Visa began to develop standards and announced the Cardholder Information Security Program (CISP) in April, 2000. These standards became required in June, 2001, for all entities that store, process or transmit Visa cardholder data.

Since that time, other credit card companies have become involved, and a new group called the Payment Card Industry Security Standards Council was formed to standardize security requirements across the entire credit card industry. The result is a new security standard called Payment Card Industry Data Security Standard (PCI-DSS or simply 'PCI') which is designed to ensure standardized compliance for multiple associations.

This document is provided to guide users of *Evosus® Business Management System* into becoming and remaining PCI compliant.

## *1.2 Why you need to be concerned about this*

Credit Card companies are requiring compliance with PCI standards for every entity that is involved in the storage, processing, or transmission of credit card information. Failure to comply can result in denial or revocation of your organization's ability to process credit cards.

Furthermore, as these standards have become widely recognized, non-compliance places your organization at risk of legal and/or civil consequences if credit card information becomes compromised.

Compliance with PCI standards is necessary whether or not you use *Evosus® Business Management System* to process transactions "online." Even if you use a POS terminal or other method to process transactions, and simply retain information in *Evosus® Business Management System*, you must be concerned about proper use of the program to maintain security and confidentiality of customer data.

As of October 1, 2008, Credit Card Processors and Bank Card Acquirers must only accept level 3 and 4 merchants that are PCI-DSS compliant or that utilize PA-DSS compliant applications.

Beginning October 1, 2009, all payment applications which are not PA-DSS compliant will be de-certified.

Beginning July 1, 2010, Credit Card Processors and Bank Card Acquirers must ensure that merchants and agents use only PA-DSS compliant applications.

### *1.3 The PCI Data Security Standard*

The "PCI-DSS" is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

To learn more about PCI, visit www.pcisecuritystandards.org.

The standard must constantly evolve in order to remain viable in today's rapidly changing internet and computing environment. Thus, the PCI-DSS will be reviewed at least every 24 months, and can be updated at any time.

*Evosus® Business Management System* Version 6.5 has been certified as compliant under the Payment Application Data Security Standard (PA-DSS) 3.2. The PA-DSS is a separate security standard that applies to software vendors that develop applications for sale to merchants to process and/or store cardholder data. Just because *Evosus® Business Management System* has been certified as PA-DSS 3.2 compliant does not automatically make you, as a merchant, PCI compliant. It *is* an important and necessary step toward that goal. Payment applications validated per the PA-DSS, when implemented in a PCI-DSS-compliant manner, will minimize the potential for security breaches leading to compromises of sensitive cardholder data, and the damaging fraud resulting from these breaches, and speed you on your way to PCI compliance.

## 2 Merchant and Requirements for Compliance

There are twelve basic requirements (organized in six areas) which a merchant must meet in order to become certified as PCI-compliant. Each of these requirements, along with POS Vendor's recommendations, is noted in this document. However, you must familiarize yourself with the details of each requirement as set forth in the PCI Data Security Standard documentation. (Refer to Section 4 "Resources" for guidance on where to get more information.) The following table lists the twelve basic requirements.

**PCI Requirements**

| PCI Topic | Basic Requirement |
|---|---|
| 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 |
| | 6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 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 |

## 3 *Evosus® Business Management System* PCI Security Practices

Because it has been certified as compliant under the PA-DSS 3.2 requirements, using *Evosus® Business Management System* as a tool will support you in meeting some of your merchant requirements to become and remain PCI-DSS compliant. However, it is important that you use the software as designed, and that you follow certain practices and procedures internally both when you install the software and as you enter transactions.

Compliance with PCI standards is necessary and you must be concerned about proper use of the program to maintain security and confidentiality of customer data. Therefore, the following sections provide guidance on how to implement and maintain the *Evosus® Business Management System* application per PA-DSS requirements (as they relate to PCI) along with other general PCI security information.

# 4 Securely implementing Evosus® Business Management System

## *4.1 Sensitive Authentication Data*

**Reference:** PA-DSS 1.1.4 Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data

### 4.1.1 Previous Versions

*Evosus® Business Management System* versions prior to release 6.5 stored some sensitive cardholder data if the Evosus Card Services by OpenEdge product was licensed and if that feature was actually used. The cardholder PAN is encrypted. In version 6.5 all the cardholder PAN is retained only if Card on File data is not migrated via the Migrate Legacy Cards of File to OpenEdge Tokens screen.

### 4.1.2 Troubleshooting

Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use. *Evosus® Business Management System* does not display sensitive cardholder or authentication data for multiple cardholders anywhere in the application or log such to the file system of computer running the application. Access to sensitive cardholder data is available only a single record at a time and only to authorized employee accounts based on application level permissions under the control of the application administrator.

## *4.2 Protect Stored Cardholder Data*

**Reference:** PA-DSS 2.0 Protect stored cardholder data

### 4.2.1 Purge Stale Cardholder Data

By default *Evosus® Business Management System* sets a sensitive cardholder data retention period of 12 months. This setting can be modified in System Parameters. Data older than the retention period may be purged by using the Secure Card Data/Encryption Key Maintenance screen. This screen is located on the Administration tab > ECS by PPI > General Setup > Secure Card Data/Encryption Key Maintenance. The purge process modifies affected records by removing the full credit card number, replacing it with a masked number having only the original first four and last four digits of the credit card number, all other characters will contain the letter ‘X’. The Secure Card Data/Encryption Key Maintenance screen affects all locations where credit card numbers are stored.

**PCI DSS Requirement 3.1** Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.

### 4.2.2 Securely Delete Cryptographic Material

During the upgrade to version 6.5 of *Evosus® Business Management System* sensitive cardholder is automatically re-encrypted with new keys that should be rotated automatically every 90 days in accord with PCI-DSS guidelines. Evosus will notify every 90 days via ‘Employee Action Item’ all employees belonging to the ‘PCI Data Security’ notification group. The encryption key used to encrypt sensitive cardholder data may be rotated by using the Secure Card Data/Encryption Key Maintenance screen. This screen is located on the Administration tab > ECS by PPI > General Setup > Secure Card Data/Encryption Key Maintenance. The encryption process modifies affected records by first decrypting the full credit card number where it is stored, then after generating a new encryption key, re-encrypting the full credit card number for storage. The Secure Card Data/Encryption Key Maintenance screen affects all locations where credit card numbers are stored.

### 4.2.3 System Backups

In order to prevent the inadvertent retention of cardholder data (albeit in an encrypted form), follow these procedures when performing system backups. Remove these tables from database containing the *Evosus® Business Management System* database:

- CardOnFiles
- CardRequests
- CardSettleRequests
- CardPPIRequests
- CustomerPayments

In addition, the data encrypting key is stored in the ‘SecurityKeys’ table. To prevent inadvertent retention of cardholder data, system backups should remove this table.

### 4.2.4 Rendering Cardholder Data

Evosus Business Management System v6.5 has two options for controlling the visibility of cardholder data stored using previous Evosus Business Management System versions (v6.0-v6.4). Below are instructions on how to configure each option (PA DSS 2.3)

1. **Customer Credit Card on File Screen-Non OpenEdge (Report)**
   This report contains a hyperlink for each row that links to the Credit Card on File Form for a single Card of File record. The ability to disable the readable cardholder data is controlled by disabling the following permission:

   *Menu Path*
   Administrator Tab > Evosus Administration > Evosus Security-Employee Level Permissions > Credit Card Processing Category

   Security Permission Setting: Can View Full Credit Card Number

2. **Merchant Credit Card Receipt (PDF)**
   The Merchant Copy receipt may optionally contain the full credit card number via a configurable system parameter. The ability to disable the readable cardholder data is controlled by setting the following parameter:

   *Menu Path*
   Administrator Tab > Evosus Administration > System > Evosus Defaults > System Parameters > Evosus Card Services (Category) > Truncate Card Number on Merchant Receipt Copy

   Parameter Value: YES

Evosus Business Management System does not output cardholder PAN outside of the application, either via reports or logging.

### 4.2.5 Access to Cryptographic Material

Evosus Business Management System is not distributed through resellers. Evosus Business Management System is not integrated through 3rd party integrators. This obviates the storage, distribution and retirement policies of cryptographic keys and management of non-Evosus cryptographic custodians. Cryptographic keys are generated, rotated and retired according to strict rules enforced by the Evosus Business Management System application only.

Root cryptographic keys are only known by the development department employees. Working cryptographic keys are generated by Evosus Business Management System and managed through the Key Rotation feature described in section 4.2.2 of this guide.

## *4.3 Secure Authentication Features*

**Reference:** PA-DSS 3.1 Secure authentication features

**Comment [A1]:** ORIGINAL NOTE FROM BARRY:
New Section Requirement for PA DSS 2.2
The following must be provided for customers and integrators/resellers:
▪Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts.
▪Confirmation that the payment application masks PAN by default on all displays.
▪Instructions on how to configure the payment application such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN (includes displays of the full PAN).
New Instructions required to meet PA DSS 2.3
The following must be provided for customers and integrators/resellers:
▪Details of any configurable options for each method used by the application to render cardholder data unreadable, and **instructions on how to configure each method for all locations where cardholder data is stored** by the payment application (per PA-DSS Requirement 2.1).
▪A list of all instances where cardholder data may be output for the customer to store outside of the payment application, and instructions that the customer is responsible for rendering PAN unreadable in all such instances.
▪Instruction that if debugging logs are ever enabled (for example, for troubleshooting purposes), and the logs include PAN, they must be protected in accordance with PCI DSS, disabled as soon as troubleshooting is complete and securely deleted when no longer needed.

**Comment [A2]:** ORIGINAL NOTE FROM BARRY:
New Instruction needed for 2.4, 2.5.1 – 2.5.7, & 2.6
The following instructions must be provided for customers and integrators/resellers:
▪Restrict access to keys to the fewest number of custodians necessary.
▪Store keys securely in the fewest possible locations and forms.

The following must be provided for customers and integrators/resellers:
▪How to securely generate, distribute, protect, change, store, and retire/replace cryptographic keys, where customers or integrators/resellers are involved in these key-management activities.
▪A sample Key Custodian Form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.

Provide instructions for customers and integrators/resellers on how to perform key-management functions including:
▪Generation of strong cryptographic keys.
▪Secure cryptographic key distribution.
▪Secure cryptographic key storage.
▪Cryptographic key changes for keys that have reached the end of their cryptoperiod.
▪Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.
▪Split knowledge and dual control for any manual clear-text cryptographic key management operations supported by the payment application.
▪Prevention of unauthorized substitution of cryptographic keys.

The following instructions must be provided for customers and integrators/resellers:
▪Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable.
... [1]

### 4.3.1 Administrative and Privileged Access to the Application

The “out of the box” installation of *Evosus® Business Management System* facilitates the use of unique user IDs and secure authentication (defined at PCI DSS Requirements 8.1, 8.2, and 8.5.8–8.5.15) for all administrative access and for all access to cardholder data. *Evosus® Business Management System* further reduces risk exposure due to storage of sensitive cardholder data by not displaying sensitive cardholder data for multiple cardholders in reports or exports. This is true for all levels of application access.

*Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the payment application.*

An employee or service provider (such as Evosus, Inc.) with knowledge of the Administrator accounts for the database engine used by *Evosus® Business Management System* could access cardholder data (albeit in an encrypted form) using management tools such as Microsoft SQL Server Studio or through report writing tools such as Crystal Reports. Therefore you should take the following precautions:

a) Change the password for the standard SQL login “sa” from the default. Also change the password for the standard SQL login used by the Evosus application (‘EvosusUser’) or confirm that this was done during installation of the Evosus Business Management System. The password may be changed through tools such as SQL Server Management Studio. To configure *Evosus® Business Management System* to use the new password click the ‘Change’ button on the Login screen.

b) Assign secure authentication to these default accounts (even if they won’t be used), and then disable or do not use the accounts. Do not disable the ‘EvosusUser’ standard SQL login as it is used.

c) You should assign secure authentication using strong passwords for employee logins in *Evosus® Business Management System* and when assigning the password for the ‘EvosusUser’ standard SQL login.

d) For further direction on how to create create PCI DSS-compliant secure authentication to access the payment application, per PCI DSS Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 *(see Appendix for details of PCI DSS Requirement 8)*

e) Changing “out of the box” installation settings for unique user IDs and secure authentication will result in noncompliance with PCI DSS.

### 4.3.2 General Non-privileged Access to the Application

Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication. PCI Data Security Standard Requirements 8.1 and 8.2

Provide instructions to customers and resellers/integrators to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data.

> **PCI DSS Requirement 8.1**: Assign all users a unique ID before allowing them to access system components or cardholder data.
>
> **PCI DSS Requirement 8.2**: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
> - Password or passphrase
> - Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

### *4.4 PA-DSS Requirement 4.0*

**Reference: PA-DSS 4.0 Log payment application activity**

The “out-of-box” implementation of *Evosus® Business Management System* logs access to the payment application including “Overrides” and cannot be disabled. The following logging events can be viewed (subject to application security) from the Master Audit Log Search screen (Administration > System > Security > Master Audit Log Search).

1) Successful or unsuccessful login
2) Encryption key rotation
3) Purge of sensitive card-holder data

The logging information available there can be exported to spreadsheet format for integration into a centralized logging system.

### *4.5 Evosus® Business Management System Versioning*

**Reference:** PA-DSS 5.5.4 Vendor’s published versioning methodology

Evosus utilizes the following software version scheme to track version of our Evosus® Business Management System application:

- Naming Convention:  Unique numeric identifier that consists of one or more sequences of numbers. Example Evosus® Business Management System v6.4.58
- Change Significance:
  - 6.4.58 - The first number sequence is incremented only when the code is completely rewritten.
  - 6.4.58 – The second number sequence is incremented when when there are major jumps in functionality such as changing the framework which

could cause incompatibility with interfacing system or major additions or revisions to a feature.

- 6.4.58 - The third number sequence is incremented when when there are minor revisions or bug fixes to existing application features.

**Comment [A3]:** ORIGINAL NOTE FROM BARRY:
New Section Requirement PA DSS 5.5.4
Provide a description of the vendor's published versioning methodology, and include guidance for the following:
▪Details of versioning scheme, including the format of the version scheme (number of elements, separators, character set, etc.).
▪Details of how security-impacting changes will be indicated by the version scheme.
▪Details of how other types of changes will affect the version.
▪Details of any wildcard elements that are used, including that they will never be used to represent a security-impacting change.

## 4.6 *Protect Wireless Transmissions*

**Reference:** PA-DSS 6.0 Protect wireless transmissions

### 4.6.1 Wireless Technology Included in or with the Payment Application

For payment applications using wireless technology, the wireless technology must be implemented securely. PCI Data Security Standard Requirements 1.2.3, 2.1.1 & 4.1.1

Evosus, Inc. does not recommend using *Evosus® Business Management System* through wireless technology.

If such is used, per PCI DSS Requirement 1.2.3 you must install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

### 4.6.2 General Use of Wireless Technology

If wireless technology is (or can be) used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (LAN) is connected to or part of the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed as well (for example, Requirements 1.2.3, 2.1.1, and 4.1.1). Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Wireless environments must be implemented and maintained per the following PCI DSS Requirements:

**PCI-DSS 1.2.3** Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

**PCI-DSS 2.1.1** For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

**PCI-DSS 4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

- *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.*
- *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*

## *4.7 Systems Connected to the Internet*

**Reference:** PA-DSS 9.0 Cardholder data must never be stored on a server connected to the Internet

Evosus, Inc. recommends that the computer hosting the Evosus database and PC running *Evosus® Business Management System* be separated from the internet via a secure firewall such as Sonicwall. Evosus Solutions, Inc. is an authorized Sonicwall reseller.

At the very least the database server should not have access to the internet. When accessed via Remote Desktop Connection the Evosus Business Management System does not require that the terminal server and the database be on the same server, nor is the database server required to be in the DMZ if one exists.

- Evosus, Inc. strongly recommends that the database server not have access to the internet. Wherever internet is accessible in the application environment *Evosus® Business Management System* should execute on a PCs or a dedicated terminal server running where the database server is a separate server or host pc not connected to the internet.

## *4.8 Secure Remote Software Updates*

**Reference:** PA-DSS 10.0 Facilitate secure remote software updates

Evosus updates its *Evosus® Business Management System* periodically. Evosus communicates the availability of new releases through our Support Center portal (https://support.evosus.com) and via email to licensed Evosus customers. When a new update is available, the installation package is automatically downloaded to the customer's application server, but not installed. Evosus customers may install the new release or optionally have Evosus to install it via Secure Remote Access.

**Comment [A4]:** ORIGINAL NOTE FROM BARRY:
The following must be provided for customers and integrators/resellers:
•How the vendor will communicate notifications of new patches and updates.

In the case where Evosus, Inc. performs the installation Evosus personnel will use secure remote access method described in section 4.9 at a mutually agreed to time.

**Reference:** PCI Data Security Standard Requirements 1.3.5 and 1.3.6

To secure such communications Evosus, Inc. recommends that the computer hosting the Evosus database be located in an internal network zone, segregated from the DMZ and other untrusted networks. The application server running *Evosus® Business Management System* should be separated from the internet via a secure firewall such as Sonicwall. Evosus Solutions, Inc. is an authorized Sonicwall reseller.

## *4.9 Secure Remote Access to Payment Application*

**Reference:** PA-DSS 11.0 Facilitate secure remote access to payment application

### 4.9.1 Multi-Factor Authentication

If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a Multi-factor authentication mechanism.

**PCI DSS Requirement 8.3:** Incorporate Multi-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.

Multi-factor authentication is defined as something you have (e.g. smartcard or token) and something you know (e.g. PIN or biometric). These two factors must be presented in conjunction with one another to authenticate to a network or system.

The recommended method for secure remote access to *Evosus® Business Management System* by Evosus personnel is Bomgar Remote Support with Bomgar Verify. Bomgar Verify employs two-factor authentication for all remote access sessions. Per PCI DSS requirement 8.3 customer employee access to *Evosus® Business Management System* requires two-factor authentication. The customer should review the various modes of remote access to *Evosus® Business Management System,* turn off any remote access solutions that do not meet the two-factor authentication requirement.

### 4.9.2 Secure Remote Access Requirements

If you use remote access software, you should follow the guidance below to use and implement remote access security features.

Note: Examples of remote access security features include:

a) Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).

b) Allow connections only from specific (known) IP/MAC addresses.

c) Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15. *(see Appendix for details on PCI DSS Requirement 8)*

d) Enable encrypted data transmission according to PCI DSS Requirement 4.1.

**PCI DSS Requirement 4.1:** Use strong cryptography and security protocols such as SSL/TLS or 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), and*
- *General Packet Radio Service (GPRS).*

e) Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13. *(see Appendix of this document for details on PCI DSS Requirement 8)*

f) Configure the system so a remote user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed.

g) Enable the logging function.

h) Restrict access to customer passwords to authorized Evosus support personnel.

i) Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5. *(see Appendix for detailed PCI DSS Requirements)*

### *4.10 Encrypt Sensitive Traffic over Public Networks*

**Reference:** PA-DSS 12.0 Encrypt sensitive traffic over public networks

*Evosus® Business Management System* sends cardholder data over public networks during the credit card authorization process. This is the only time cardholder data is sent outside your private network. *Evosus® Business Management System* uses TLS 1.2 and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during that transmission.

*Evosus® Business Management System* never sends unencrypted PANs using messaging technologies such as e-mail, instant messaging, or chat.

If for trouble-shooting purposes unencrypted credit card numbers need to be communicated to Evosus support personnel, Evosus recommends that this be done over the telephone and not via email, instant messaging or chat.

### *4.11 Encrypt all Non-console Administrative Access*

**Reference:** PA-DSS 13.0 Encrypt all non-console administrative access

13.1 Instruct customers to encrypt all non-console administrative access using technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

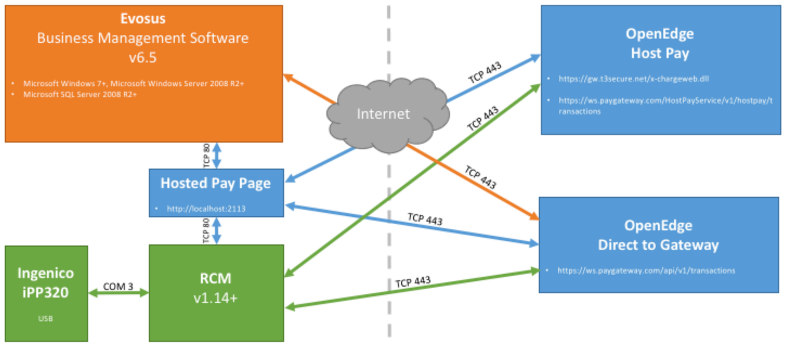
PCI Data Security Standard Requirement 2.3

Telnet or rlogin must never be used for administrative access.

- *Evosus® Business Management System* does not facilitate non-console remote access. Non-console remote access to a customer server is only provided the installed Operating System where *Evosus® Business Management System* is installed. Such access should be secured by multi-factor authentication and encrypted using technologies such as SSH, VPN, or TLS 1.2. *Evosus® Business Management System* does not prevent the implementation of multi-factor auth to the OS supporting the application.

Components Involved in Cardholder Data Communication

**Evosus BMS v6.5 Payment Network Communications Diagram**


Evosus
Business Management Software
v6.5
Microsoft Windows 7+, Microsoft Windows Server 2008 R2+
Microsoft SQL Server 2008 R2+
Internet
OpenEdge
Host Pay
https://gw.t3secure.net/x-chargeweb.dll
https://ws.paygateway.com/HostPayService/v1/hostpay/transactions
TCP 443
TCP 443
TCP 80
Hosted Pay Page
http://localhost:2113
TCP 443
TCP 443
OpenEdge
Direct to Gateway
https://ws.paygateway.com/api/v1/transactions
TCP 80
Ingenico
iPP320
USB
COM 3
RCM
v1.14+
TCP 443

**Comment [A5]:** ORIGINAL NOTE FROM BARRY:
Following additional information must be included"
Document all required protocols, services, components, and dependent software and hardware that are necessary for any functionality of the payment application. Example include: Supported O/S, supported databases software, and PINPADS.

Must also define all communication TCP ports to used for transmission of CHD.

New Section requirement for 12.1 & 12.1.1
If the payment application facilitates non-console administrative access, include instructions on how to configure the application to use strong cryptography for encryption of all non-console administrative access to payment application or servers in cardholder data environment. If application does not support non-console access, must not prevent the implementation of multi-factor auth to the OS supporting the application.

# 5 Appendix

## *PCI-DSS Requirement 8*

### Assign a Unique ID to each Person with Computer Access

**PCI DSS 8.1:** Assign all users a unique ID before allowing them to access system components or cardholder data.

**PCI DSS 8.2:** In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

- Password or passphrase
- Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)

**PCI DSS 8.3:** Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
**PCI DSS 8.4:** Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations and Acronyms).

**PCI DSS 8.5:** Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:

**PCI DSS 8.5.1:** Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

**PCI DSS 8.5.2:** Verify user identity before performing password resets

**PCI DSS 8.5.3:** Set first-time passwords to a unique value for each user and change immediately after first use

**PCI DSS 8.5.4:** Immediately revoke access for any terminated users

**PCI DSS 8.5.5:** Remove/disable inactive user accounts at least every 90 days.

**PCI DSS 8.5.6:** Enable accounts used by vendors for remote maintenance only during the time period needed

**PCI DSS 8.5.7:** Communicate password procedures and policies to all users who have access to cardholder data

**PCI DSS 8.5.8:** Do not use group, shared, or generic accounts and passwords

**PCI DSS 8.5.9:** Change user passwords at least every 90-days

**PCI DSS 8.5.10:** Require a minimum password length of at least seven characters

**PCI DSS 8.5.11:** Use passwords containing both numeric and alpha characters

**PCI DSS 8.5.12:** Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

**PCI DSS 8.5.13:** Limit repeated access attempts by locking out the user ID after not more than six attempts.

**PCI DSS 8.5.14:** Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

**PCI DSS 8.5.15:** If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.

**PCI DSS 8.5.16:** Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.

**Page 8: [1] Commented** **Author**

ORIGINAL NOTE FROM BARRY:

## New Instruction needed for 2.4, 2.5.1 – 2.5.7, & 2.6

The following instructions must be provided for customers and integrators/resellers:

- Restrict access to keys to the fewest number of custodians necessary.
- Store keys securely in the fewest possible locations and forms.

The following must be provided for customers and integrators/resellers:

- How to securely generate, distribute, protect, change, store, and retire/replace cryptographic keys, where customers or integrators/resellers are involved in these key-management activities.
- A sample Key Custodian Form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.

Provide instructions for customers and integrators/resellers on how to perform key-management functions including:

- Generation of strong cryptographic keys.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.
- Cryptographic key changes for keys that have reached the end of their cryptoperiod.
- Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.
- Split knowledge and dual control for any manual clear-text cryptographic key management operations supported by the payment application.
- Prevention of unauthorized substitution of cryptographic keys.

The following instructions must be provided for customers and integrators/resellers:

- Procedures detailing how to use the tool or procedure provided with the application to render cryptographic material irretrievable.
- That cryptographic key material should be rendered irretrievable whenever keys are no longer used and in accordance with key-management requirements in PCI DSS.
- Instructions on how to re-encrypt historic data with new keys, including procedures for maintaining security of clear-text data during the decryption /re-encryption process.