NODUS® Technologies, Inc.

ePay PA-DSS Implementation Guide

For ePay Advantage version 6 with PA-DSS 3.2

March, 2016 – Document Version 1.0

ePay Advantage
Integrated Bill Pay Portal

Table of Contents

Introduction

The Payment Application Data Security Standards (PA-DSS) define security requirements and assessment procedures for software vendors of payment applications.

The objective of this document is to address how the Nodus Technologies' ePay Advantage (ePay) solution meets all the PA-DSS v3.2 requirements and to provide customers, partners and integrators with specific guidelines on how to implement ePay Advantage in a PA-DSS compliant fashion.

Nodus Technologies strongly recommends that partners, integrators and customers follow these guidelines without exception. Failure to follow these guidelines may result in the customer environment falling into a PCI non-compliant status and increases the possibility of cardholder data being compromised.

This guide does not take into account PCI DSS requirements for anything that is not covered by ePay Advantage application. Obtaining PCI-DSS Compliance is the customer's responsibility by using PCI compliant server architecture with proper hardware & software configurations and access control procedures. The PCI-DSS requirements document can also be obtained from the above link.

For more information regarding how these standards apply to the ePay installation and configuration, contact Nodus Support at (909) 482-4701 Option 2.

Abbreviations

The following abbreviations are utilized within this document.

Abbreviation	Description
SAD	Sensitive Authentication Data - Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks
PAN	Primary Account Number
PCI-DSS	Payment Card Industry Data Security Standard
PA-DSS	Payment Application Data Security Standard
CDE	Cardholder Data Environment

PA-DSS 3.2 Documentation

This guide is written with direct references to the PA-DSS 3.2 Standards documentation. A full copy of this document can be obtained from the PCI Security Standards website at the URL below:

https://www.pcisecuritystandards.org/document_library

About ePay Advantage

Nodus ePay Advantage (ePay) offers the latest online payment technology for enterprises to streamline electronic bill payment and presentment. EPay Advantage offers real-time payment processing for both credit card and eCheck transactions while ensuring the highest standards of security are addressed.

Installation and Usage of ePay Advantage

There are separate documents for the installation or usage of ePay Advantage. These documents can be obtained from the below links. The installation guide will cover deployment architecture, server requirements and server configurations for ePay.

Installation Guide	http://www.nodus.com/documentation/ePay-6-Installation-Guide.pdf
User Guide	http://www.nodus.com/documentation/ePay-6-User-Guide.pdf

Transaction Processing Options

To address different security needs for different organizations, ePay supports multiple options for the processing of transactions and credit card storage. It is important to be aware of which payment option will be in use for the ePay installation to determine the relevant guidelines referenced in this document.

PayFabric® Option

The **PayFabric® Option** utilizes the Nodus Cloud Processing Solution, PayFabric®, to dramatically reduce the scope of PCI compliance by removing the credit card storage, the credit card transmission and potentially the credit card entry point from the merchant’s environment. The PayFabric® Option moves all the credit card entry and processing to the PayFabric® cloud to relieve ePay and the merchant from any contact with the sensitive credit card number. This option supports multiple payment gateways and PayFabric® can easily be integrated with other applications to utilize the stored account information in the Payfabric® cloud across applications.

Tokenization Option

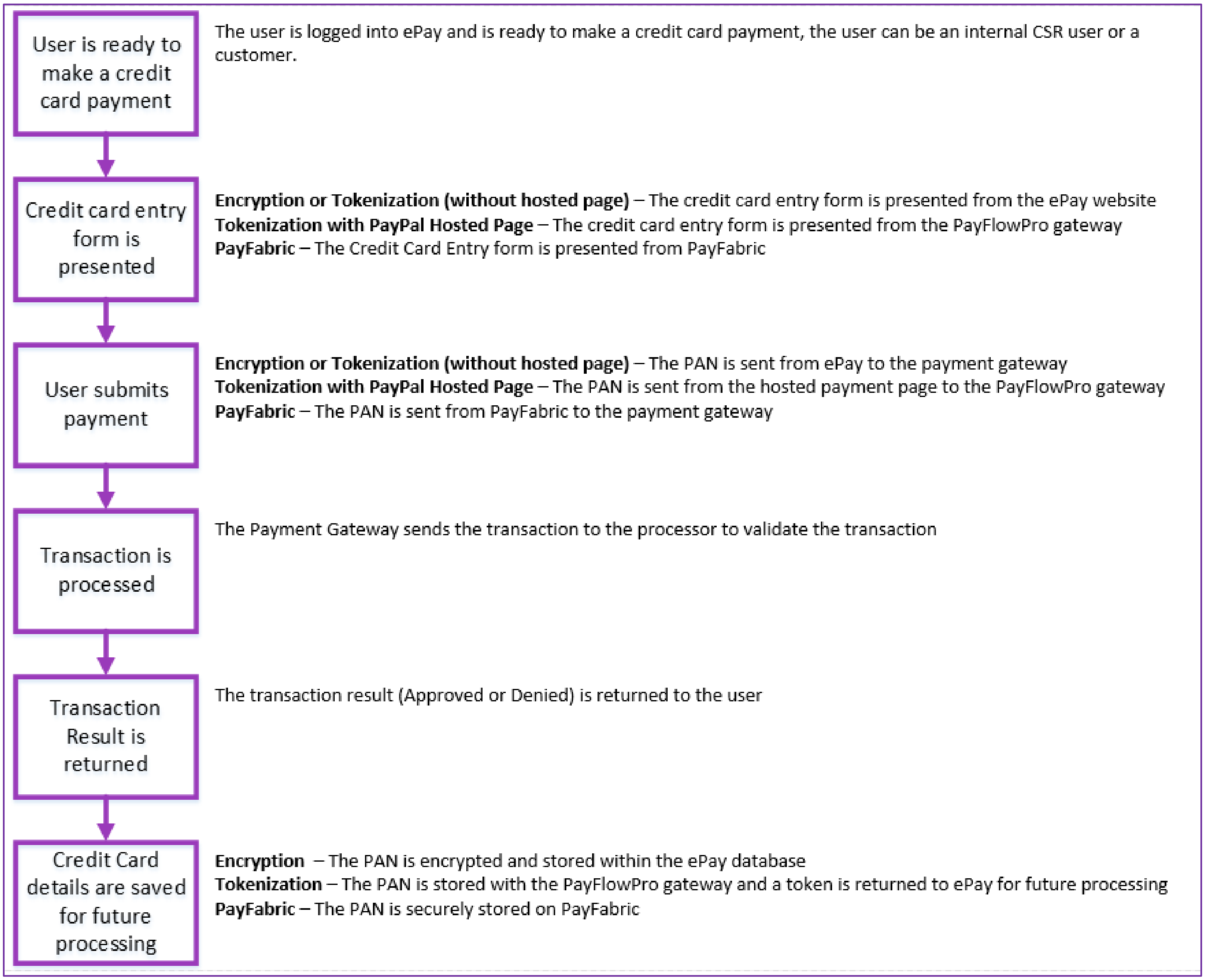
The **Tokenization option** utilizes a service from the PayPal PayFlowPro Payment Gateway account where the Payment Gateway will manage credit card numbers provide ePay with a token value to symbolize each credit card number. EPay will store the token instead of the credit card number for future processing. This option can help merchants reduce the scope of PCI Compliance since Credit Cards are no longer stored in the company databases. The Tokenization Option is available for companies using the PayPal PayFlowPro Payment Gateway when the account has been setup through Nodus.

Encryption Option

The **Encryption Option** is where the credit card information is stored (in encrypted format) on local premise. With the Encryption option, ePay is bundled with Nodus Encryption, a service that encrypts credit cards in a format that has been approved to meet PCI Data Security Standards. This method of credit card storage supports multiple Payment Gateways and Processors.

Transaction Process Flow Diagram

Below is a diagram detailing how a credit card transaction occurs within ePay. This process does vary based on the Transaction Processing Option


User is ready to make a credit card payment
Credit card entry form is presented
User submits payment
Transaction is processed
Transaction Result is returned
Credit Card details are saved for future processing

The user is logged into ePay and is ready to make a credit card payment, the user can be an internal CSR user or a customer.

Encryption or Tokenization (without hosted page) – The credit card entry form is presented from the ePay website
Tokenization with PayPal Hosted Page – The credit card entry form is presented from the PayFlowPro gateway
PayFabric – The Credit Card Entry form is presented from PayFabric

Encryption or Tokenization (without hosted page) – The PAN is sent from ePay to the payment gateway
Tokenization with PayPal Hosted Page – The PAN is sent from the hosted payment page to the PayFlowPro gateway
PayFabric – The PAN is sent from PayFabric to the payment gateway

The Payment Gateway sends the transaction to the processor to validate the transaction

The transaction result (Approved or Denied) is returned to the user

Encryption – The PAN is encrypted and stored within the ePay database
Tokenization – The PAN is stored with the PayFlowPro gateway and a token is returned to ePay for future processing
PayFabric – The PAN is securely stored on PayFabric

About Credit Card Advantage

EPay Advantage with Dynamics GP integrates to Credit Card Advantage for additional processing needs. If the Encryption Option is enabled, encrypted PAN values are sent and shared with Credit Card Advantage. Please review the PA-DSS Implementation Guide for Credit Card Advantage to ensure the best practices are met for Credit Card Advantage usage. Please contact Nodus Technologies for a copy of this document.

PA-DSS 3.2 Requirements

This section of the guide will explain how ePay meets the PA-DSS 3.2 requirements and the customer's responsibility in ensuring they manage the ePay Advantage application properly. This section directly references the requirements of the PA-DSS 3.2 Standards Documentation.

1 - Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

1.1

(Aligns with PCI DSS Requirement 3.2)

Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

Sensitive authentication data includes the data as cited in the following Requirements 1.1.1 through 1.1.3 from the PA-DSS 3.2 Standard

Software Vendor Conformance:
EPay Advantage never stores sensitive authentication data after authorization even if encrypted.

Guidance for Customers/Integrators:-
Customers should never store or capture sensitive authentication data after authorization. For ePay Advantage troubleshooting, only the application and system security log files are required. PAN and sensitive authentication data are not captured in the application logs or system security logs.

1.1.1, 1.1.2, 1.1.3

(Aligns with PCI DSS Requirement 3.2.1, 3.2.2, 3.2.3)

After authorization, do not store,

- *Full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.*
- *Card Verification value or Code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.*
- *Personal identification number (PIN) or the encrypted PIN block*

Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- *The accountholder's name,*
- *Primary account number (PAN),*
- *Expiration date, and*
- *Service code*

To minimize risk, store only those data elements needed for business

Software Vendor Conformance:

EPay Advantage does not store any sensitive authentication data such as Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks after authorization. Any ePay Advantage log kept does not contain any sensitive authentication data. Also, all the memory locations initialized with the above data are rewritten with NULL as soon as the transaction is completed. No sensitive authorization data is ever stored on the hard drive.

Guidance for Customers/Integrators:

Customer must NOT in any manner (electronic or written) store Sensitive data (full magnetic Stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data) post Authentication.

1.1.4

(Aligns with PCI DSS Requirement 3.2)

Securely delete any track data (from the magnetic stripe or equivalent data contained on a chip), card verification values or codes, and PINs or PIN block data stored by previous versions of the payment application

Note: This requirement applies only if previous versions of the payment application stored sensitive authentication data.

Software Vendor Conformance:

This requirement is not applicable as ePay Advantage has never stored sensitive authentication data

Guidance for Customers/Integrators:

If using a different payment processing application other than ePay previously, it is required to securely remove any unencrypted historical data containing magnetic stripe information, card validation codes, PINs, or PIN blocks stored by that application in order to be compliant with PCI-DSS requirements.

1.1.5

(Aligns with PCI DSS Requirement 3.2)

Do not store sensitive authentication data on vendor systems. If any sensitive authentication data (pre-authorization data) must be used for debugging or troubleshooting purposes, ensure the following:

Sensitive authentication data is collected only when needed to solve a specific problem.

- *Such data is stored in a specific, known location with limited access.*
- *The minimum amount of data is collected as needed to solve a specific problem.*
- *Sensitive authentication data is encrypted with strong cryptography while stored.*
- *Data is securely deleted immediately after use, including from:*
    - *Log files*
    - *Debugging files*
    - *Other data sources received from customers.*

Software Vendor Conformance:

EPay Advantage does not collect or gather any SAD from its customers for any troubleshooting purposes.

Guidance for Customers/Integrators:

Customers are advised not to send any of the SAD to Nodus Technologies or any partners for troubleshooting purposes of any transactions or disputes.

2 Protect Stored Card Holder Data

PA-DSS requirement 2 is concerned with stored card holder data in the ePay environment. It is important to note that ePay with the Encryption Option enabled securely stores card holder data. EPay with the PayFabric or Tokenization options do not store Card Holder data in the ePay environment and the card holder data is stored in the PayFabric Cloud or the PayFlowPro payment gateway. PA-DSS requirement 2 is not relevant with the PayFabric or Tokenization options enabled for ePay.

2.1

(Aligns with PCI DSS Requirement 3.1)

- *Secure deletion of cardholder data after expiration of customer-defined retention period*
- *A list of all locations where the payment application stores cardholder data (so that customer knows the locations of data that needs to be deleted).*
- *Instructions on how to securely delete cardholder data stored by the payment application.*

Software Vendor Conformance:

It is required by Requirement 3.1 of the PCI-DSS that a data classification policy is to be maintained, which takes into consideration the storage time of cardholder information as per business requirements. Customers are hereby instructed to maintain a comprehensive set of data classification, data retention and data disposal policies and procedures which dictate the amount of time cardholder information is to be stored, the storage area of cardholder information and the methods for the secure disposal of cardholder information.

EPay Advantage with the Encryption Option enabled stores the cardholder's primary account number in an encrypted/hashed method in the location mentioned in the below Card Holders data storage matrix table.

Card Holders Data Matrix

Database Name	Table Name	Column Name	SAD Stored	Protection Mechanism
ePay Database	ExtentionData	RecordValue	No	Nodus Encryption

Steps for Secure Deletion:

The National Institute for Standards and Technology (NIST) has published a detailed document 800-88 which provides the best practices for secure disposal of highly sensitive information.

http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50819

For secure deletion a third party data erasure tool should be utilized to ensure data is properly cured. A list of possible tools for data deletion can be found at the below link. Please not that Nodus Technologies does not endorse or has tested any of these solutions:

https://en.wikipedia.org/wiki/List_of_data-erasing_software

Guidance for Customers/Integrators:

Securely delete the card holder data post the retention period or when no longer required for legal, regulatory, or business purposes.

2.2

(Aligns with PCI DSS Requirement 3.3)

Mask PAN when displayed (the first six (6) and last four (4) digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN

Software Vendor Conformance:

In ePay Advantage, the PAN is displayed in masked (only last 4 digits are displayed) in the screens and reports. The full PAN is not available to be viewed from ePay Advantage.

Guidance for Customers/Integrators:

None, the PAN can only be viewed in a masked form in ePay.

2.3

(Aligns with PCI DSS Requirement 3.4)

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches:

- *One-way hashes based on strong cryptography (hash must be of the entire PAN)*
- *Truncation (hashing cannot be used to replace the truncated segment of PAN)*
- *Index tokens and pads (pads must be securely stored)*
- *Strong cryptography with associated key-management processes and procedures.*

Software Vendor Conformance:

EPay Advantage with the Encryption Option enabled uses strong cryptography and key management process to protect and store the cardholder's data (PAN) in an encrypted method in the location as mentioned in the Card Holders Data Matrix table. No PAN is stored in or outside the application in clear text. EPay uses the AES 256-bit encryption method for making the PAN unreadable and secure.

Configuration:

ePay Advantage with the Encryption Option enabled utilizes the Nodus Encryption utility for Encryption of PAN values. The Encryption Option will be automatically enabled based on the registration key provided by Nodus Technologies.

Guidance for Customers/Integrators:

Card holder data is encrypted and stored in ePay Advantage. Never record the cardholder information either in electronic format or on a physical object.

2.4

(Aligns with PCI DSS Requirement 3.5)

Payment application must protect keys used to secure cardholder data against disclosure and misuse.

Software Vendor Conformance:

The Nodus Encryption application handles the DEK (Data Encrypting Key) and KEK (Key Encrypting Key) in the secure manner. DEK is stored in the encrypted format in the NodusEncryption database and KEK is stored separately in the NodusEncryptionToken database. Both DEK and KEK have an equal cryptographic strength and protection

DEK Encryption algorithm	Microsoft Crypto API's AES 256 bit Encryption
DEK Storage path/location/container	NodusEncryption database
KEK Encryption algorithm	Microsoft Crypto API's AES 256 bit Encryption
KEK Storage path /location / container	NodusEncryptionToken database

Guidance for Customers/Integrators:

Designated key custodian from the customer end is solely responsible for maintaining the encryption keys in secure manner. DEK/KEK is to be changed at least once annually.

2.5

(Aligns with PCI DSS Requirement 3.6)

Payment application must implement key- management processes and procedures for cryptographic keys used for encryption of cardholder data, including at least the following (PA-DSS 2.5.1 – 2.5.7):

- *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 crypto period*
- *Retirement or replacement of keys*
- *Enforcement of split knowledge and dual control if the payment application supports manual clear-text cryptographic key-management operations*
- *Prevention of unauthorized substitution of cryptographic keys*
- *A sample Key Custodian Form for key custodians to acknowledge that they understand and accept their key-custodian responsibilities*

Software Vendor Conformance:

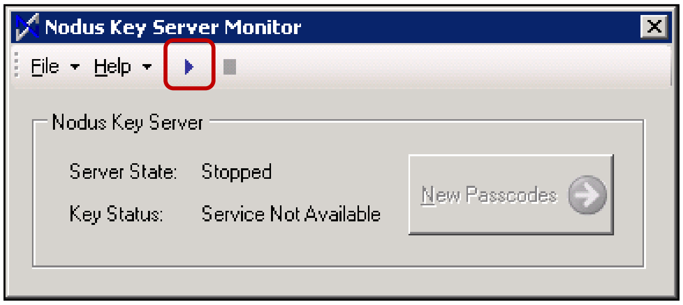
Nodus Encryption uses strong cryptography and key management process in securing the PAN. The application uses the 256-bit AES encryption method for encrypting the PAN data.

2.5.1

Generation of strong cryptographic keys

Initial Generation of Key Encrypting Key (KEK) and Data Encrypting Key (DEK)

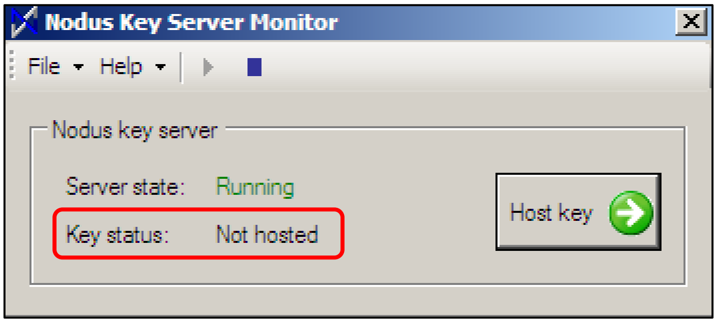
1. Log onto Key Server
2. Open the **Nodus Key Server Monitor** from the Start menu (Start > All Programs > Nodus > Nodus Encryption > Nodus Key Server Monitor)
3. Initially after the Nodus Key Server Monitor opens, the 'Key Status' should display **Service Not Available** and 'Server State' should display as **Stopped**.
4. Start the Key Server service by clicking the blue triangle icon



Server State: Stopped

Key Status: Service Not Available

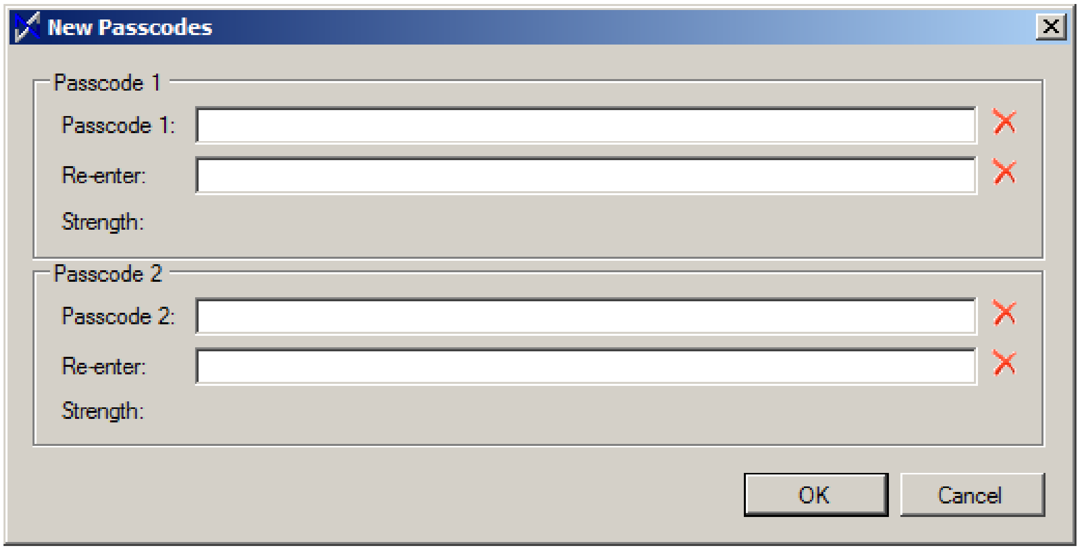
5. The 'Server State' should change to **Running** and the 'Key Status' should display as **Not Hosted**



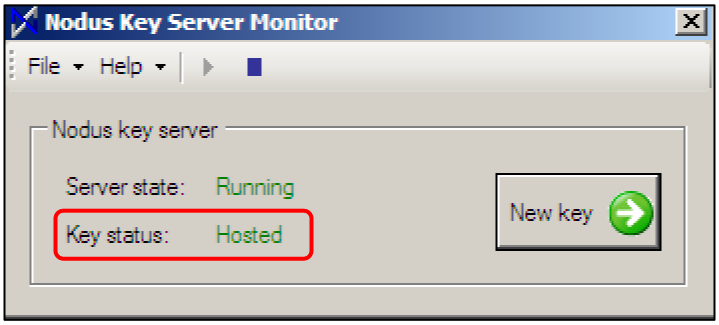
Server state: Running

Key status: Not hosted

6. Click the **Host key** button to open the 'New Passcodes' window



7. Enter the passcodes in the **Passcode 1** and **2** textboxes. The red X will change to a green checkbox if the passwords are strong enough. These passwords should be separately and securely kept with two different key custodians within the organization.
8. Click the **OK** button and the 'Key Status' should change to **Hosted.** At this time both the KEK and the DEK will be generated.



Server state: Running
Key status: Hosted

2.5.2

Secure cryptographic key distribution

The DEK is utilized by ePay with the encryption option enabled for encryption and decryption of credit card values. The DEK can only be obtained by ePay if the KEK has been hosted using the passwords provided by the two separate key custodians within the organization. Both the decrypted DEK and KEK values are never visible to a user.

2.5.3

Secure cryptographic key storage

Storage of Data Encrypting Key (DEK) and the Key Encrypting Key (KEK)

The DEK is securely stored within the Nodus Encryption database and can only be decrypted by the KEK. The KEK is generated from the dual passcodes that should be securely kept with two separate key custodians within the organization. The KEK is only kept in the temporary memory in the memory

(RAM). When the Nodus Encryption KEK service is stopped, such as when the system is rebooted, the two passwords must be entered again to generate the KEK again.

2.5.4

Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57.) Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone's obtaining the encryption keys, and using them to decrypt data.

The Nodus Encryption service will automatically rollover the encryption key on an annual basis. See below requirement 2.5.5 for instructions to manually change the encryption keys.

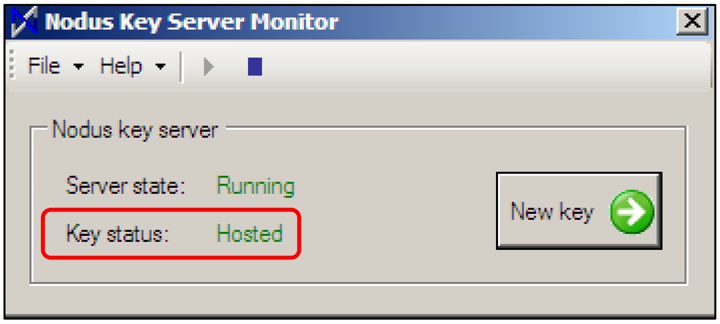
2.5.5

Retirement or replacement of keys (for example: by archiving, destruction, and/or revocation as applicable) as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component, etc.) or keys are suspected of being compromised.

- Key Rollover/ Key Change is done annually using the Nodus Encryption service and is done by rolling over the KEK. The DEK will be re-encrypted using the new KEK during the key rollover process. This is also applicable for the KEK key change process if the KEK is compromised.
- All the old historical data will be decrypted with the Old DEK and re-encrypted with the new DEK by the Nodus Encryption Rotator service

Generating a new Key Encryption Key (KEK)

1. From the Key Server, open the **Nodus Key Server Monitor** from the Start Menu (Start > All Programs > Nodus Tech > Nodus Encryption > Nodus Key Server Monitor)
2. The Key Status should display as **Hosted**. Host the key if it not yet hosted.



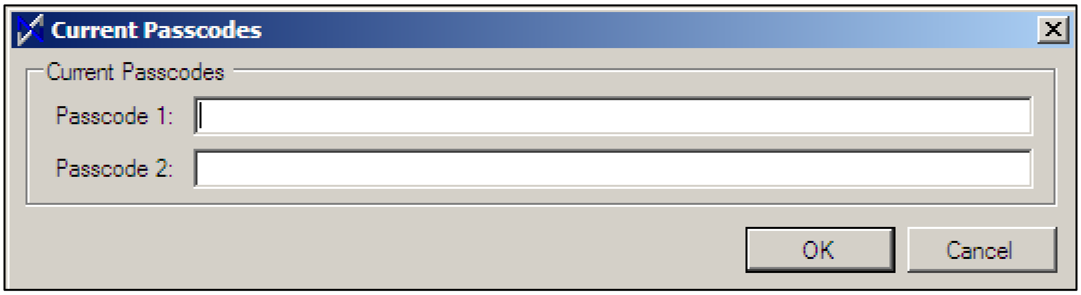
Nodus Key Server Monitor

Nodus key server

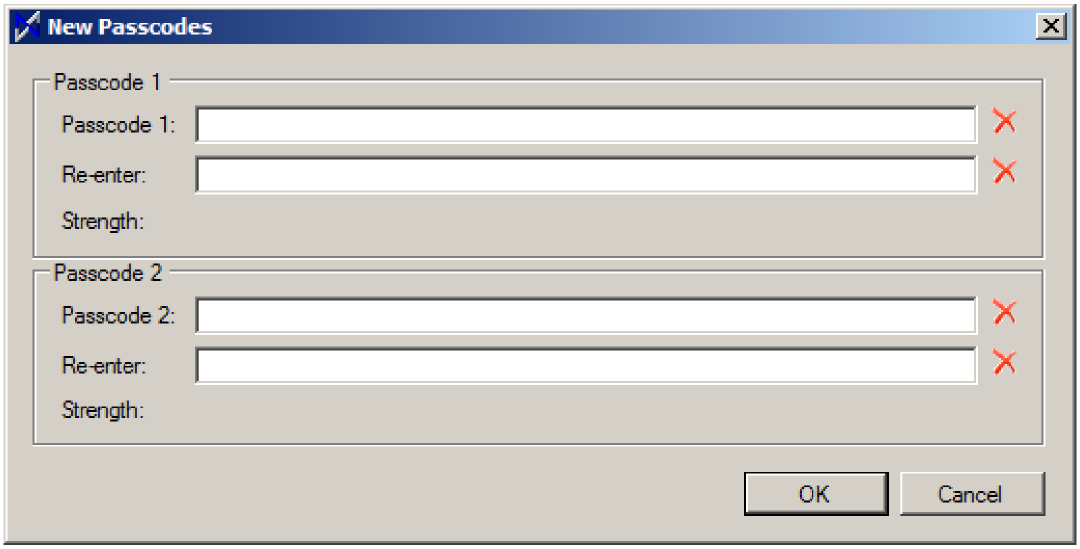
Server state: Running

Key status: Hosted

3. Click the **New key** button on the Nodus Key Server Monitor window and the 'Current Passcodes' window will open



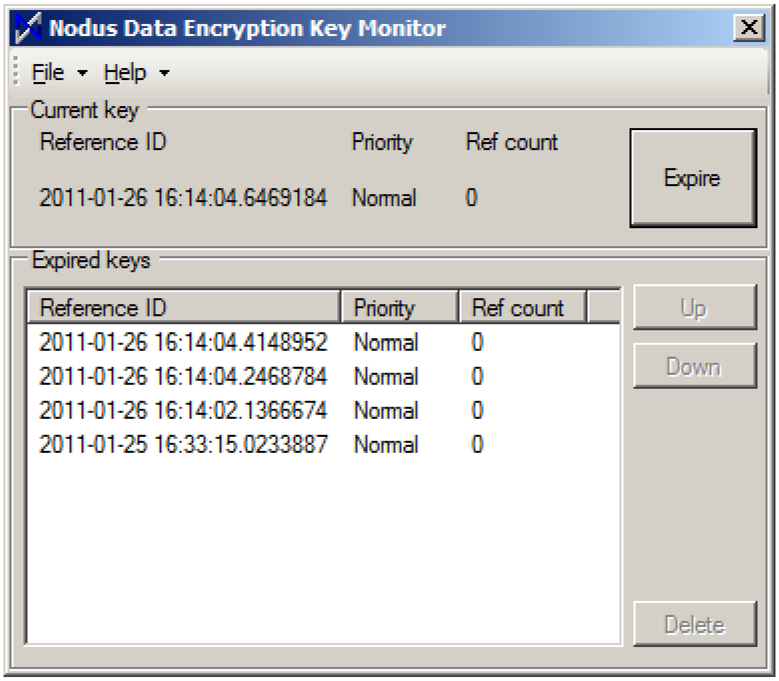
4. Enter the original Passcode 1 and Passcode 2 in the appropriate text boxes
5. Click the **OK** button and the 'New Passcodes' window will open



6. Enter the new passcodes in the **Passcode 1** and **2** textboxes. The red X will change to a green checkbox if the passwords are strong enough. These passwords should be separately and securely kept with two different key custodians within the organization.
7. Click the **OK** button to return the Key Server Monitor. At this time a new KEK will be generated and the DEKs will be encrypted using the new KEK.

Generating a new Data Encryption Key (DEK)

1. From the Key Server, open the **Nodus Data Encryption Key Monitor** from the Start Menu (Start > All Programs > Nodus Tech > Nodus Encryption > Nodus Data Encryption Key Monitor)
2. In the 'Nodus Data Encryption Key Monitor' window, click the **Expire** button to generate a new DEK. The 'Current Key' will move into the 'Expired Keys' list
3. In the evening, the Nodus Encryption Rotator service will decrypt encrypted values using the expired DEK and encrypt the value again using the current DEK.



Current key

Reference ID	Priority	Ref count
2011-01-26 16:14:04.6469184	Normal	0

Expired keys

Reference ID	Priority	Ref count
2011-01-26 16:14:04.4148952	Normal	0
2011-01-26 16:14:04.2468784	Normal	0
2011-01-26 16:14:02.1366674	Normal	0
2011-01-25 16:33:15.0233887	Normal	0

Deleting a Data Encryption Key

1. From the Key Server, open the **Nodus Data Encryption Key Monitor** from the Start Menu (Start > All Programs > Nodus Tech > Nodus Encryption > Nodus Data Encryption Key Monitor)
2. In the 'Nodus Data Encryption Key Monitor' window, click the expired key that should be deleted.
3. A key that is set to be deleted should have a 'Ref count' of zero. If the 'Ref Count' is not zero, then there are still encrypted values that are encrypted using this DEK value. Deleting this DEK will make all encrypted values using this DEK unable to be decrypted. Ensure the Nodus Encryption Rotator is running and has had the opportunity to rotate encrypted values to the new key before deleting.
4. Click the **Delete** button to delete the Expired Key.

2.5.6

If the payment application supports manual clear-text cryptographic key-management operations, these operations must enforce split knowledge and dual control.

Guidance for Customers/Integrators:

ePay and the Nodus Encryption utility do not support manual clear-text cryptographic key management operations. However, two key custodians are needed for maintaining the split knowledge of the passcodes to generate the KEK. The two passcodes should not be stored in the same location and never be accessible from a single person in the organization.

2.5.7

Prevention of unauthorized substitution of cryptographic keys

Software Vendor Conformance:

The two Encryption Passcodes are utilized to generate the KEK, the KEK is utilized to decrypt the DEK, and the DEK is needed to decrypt the encrypted values in the database. Substitution of any of these values would result in the encrypted values being unable to be decrypted.

Guidance for Customers/Integrators:

Customers are responsible for Rotating Cryptographic Keys (DEK and KEK) and changing the Key passwords on a regular basis (At least annually once). The keys must be retired or replaced when the integrity of the key has been weakened or there is a known compromise of key and ensure that retired or replaced cryptographic keys are not used for encryption process

2.6

(Aligns with PCI DSS Requirement 3.6)

Render irretrievable any cryptographic key material or cryptogram stored by the payment application, in accordance with industry-accepted standards.

These are cryptographic keys used to encrypt or verify cardholder data.

Note: This requirement applies only if the payment application uses or previous versions of the payment application used cryptographic key materials or cryptograms to encrypt cardholder data.

Software Vendor Conformance:

The DEK value can be manually deleted using the previously referenced steps for Deleting a Data Encryption Key noted in section 2.5.5. Deletion of old cryptographic material is at the customers' discretion.

Guidance for Customers/Integrators:

Customers are responsible for Rotating Cryptographic Keys (DEK and KEK) and changing the Key store password on a regular basis (At least annually once)

3 Provide secure authentication features

3.1

(Aligns with PCI DSS Requirement 8.1 and 8.2)

The payment application must support and enforce the use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data. Secure authentication must be enforced to all accounts generated or managed by the application by the completion of installation and for subsequent changes after installation.

The application must enforce 3.1.1 through 3.1.11 below:

Software Vendor Conformance:

The ePay Advantage by default supports creation of unique user id and secure authentication for all administrative access and for all access to cardholder data. All the user accounts generated or managed by the application by the completion of installation and for subsequent changes after installation prompts for user id and password for secure authentication

3.1.1

(Aligns with PCI DSS Requirement 2.1)

The payment application does not use (or require the use of) default administrative accounts for other necessary software (for example, the payment application must not use the database default administrative account).

Software Vendor Conformance:
EPay Advantage does not require the use of default administrative account for any functioning of the application.

3.1.2

(Aligns with PCI DSS Requirement 2.1)

The application must enforce the changing of all default application passwords for all accounts that are generated or managed by the application, by the completion of installation and for subsequent changes after installation. This applies to all accounts, including user accounts, application and service accounts, and accounts used by the vendor for support purposes.

Software Vendor Conformance:
EPay Advantage by default enforces changing of all default application passwords generated or managed by the application, by the completion of installation. Once the user logs in with the unique user id and default password in the application, the application forces the user to change the password at first login.

3.1.3

(Aligns with PCI DSS Requirements 8.1.1)

The payment application assigns unique IDs for user accounts

Software Vendor Conformance:
EPay Advantage by defaults assigns a unique user id for each individual application user

3.1.4

(Aligns with PCI DSS Requirements 8.2)

The payment application employs at least one of the following methods to authenticate all users:

- *Something you know, such as a password or passphrase*
- *Something you have, such as a token device or smart card*
- *Something you are, such as a biometric.*

Software Vendor Conformance:
EPay Advantage requires each and every user to possess a valid username and password to authenticate to the system and provide access to the application based on the success / failure of authentication.

3.1.5

(Aligns with PCI DSS Requirement 8.5)

The payment application does not require or use any group, shared, or generic accounts and passwords.

Software Vendor Conformance:

EPay Advantage does not require or encourage the use of group, shared or generic accounts and passwords. All the users of the application are provided with the unique user ID and password.

Guidance for Customers/Integrators:

Customers should not to share their user account information among the company and to keep it confidential with them

3.1.6

The payment application requires that passwords meet the following:

- *Require a minimum length of at least seven characters.*
- *Contain both numeric and alphabetic characters.*

Alternatively, the passwords/phrase must have complexity and strength at least equivalent to the parameters specified above.

Software Vendor Conformance:

In ePay Advantage password complexity is enabled by default. A password should contain at least 7 alphanumeric characters.

3.1.7

(Aligns with PCI DSS Requirement 8.2.4)

The payment application requires changes to user passwords at least once every 90 days.

Software Vendor Conformance:

EPay Advantage application forces the user to change the application user account password every 90 days. Password expiry settings are configurable. It allows the application administrator to configure password expiry days lesser than 90 days but not greater than 90.

3.1.8

(Aligns with PCI DSS Requirement 8.2.5)

The payment application keeps password history and requires that a new password is different than any of the last four passwords used.

Software Vendor Conformance:

EPay Advantage by default keeps the last 4 password in history, so that the users new password cannot be the last 4 used passwords.

3.1.9

(Aligns with PCI DSS Requirement 8.1.6)

The payment application limits repeated access attempts by locking out the user account after not more than six logon attempts.

Software Vendor Conformance:

EPay Advantage by default locks the application user account after the six invalid login attempts. All the invalid attempts are logged with the User Account Name, Date & Time, IP Address in the audit log file.

3.1.10

(Aligns with PCI DSS Requirement 8.1.7)

The payment application sets the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

Software Vendor Conformance:

EPay Advantage's default lockout duration is 30 minutes or until the administrator enables the user id. It allows only one attempt to login after 30 mins of automatic account lockout.

3.1.11

(Aligns with PCI DSS Requirement 8.1.8)

If a payment application session has been idle for more than 15 minutes, the application requires the user to re-authenticate to re-activate the session.

Software Vendor Conformance:

EPay Advantage's default session idle time out is configured as 15 minutes. Once the session is timed out it will prompt the user to login again with their username and password.

3.2

(Aligns with PCI DSS Requirement 8.1 and 8.2)

Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication

Software Vendor Conformance:

EPay Advantage application supports customer use of unique id's and secure authentication for user accounts and password used to access PCs, servers, and databases. It does not require the default administrator password for database/system logins.

Guidance for Customers/Integrators:

Customers are instructed to create and use the unique user id (identification) and password (secure authentication) in all the PC's, Servers, systems and databases used for access to/with the payment application and to implement the controls in the environment as per the PCI-DSS requirements (8.1, 8.2 and 8.5, 8.6)

Customers are instructed to change the default account password of databases during the installation or post the installation. If built-in user accounts such as "sys" or "system" of database is used by the application then its default password should be changed and new password complexity should meet the PCI-DSS Requirement 8.2.3

Customers are responsible and required to maintain the PCI-DSS compliant environment on which PA-DSS application is hosted. All the PCI-DSS Controls should be implemented and regular review / assessment should be conducted to ensure the proper functioning of the controls.

3.3

(Aligns with PCI DSS Requirement 8.2.1)

Secure all payment application passwords (including passwords for user and application accounts) during transmission and storage.

The payment application must,

PA-DSS Requirement 3.3.1 & 3.3.2:

- *Render all payment application passwords unreadable during transmission & storage using strong cryptographic algorithm and based on approved standards.*
- *Each password must have a unique input variable that is concatenated with the password before the cryptographic algorithm is applied*

Software Vendor Conformance:

EPay Advantage renders passwords unreadable all times in the rest and transit. EPay uses one way strong cryptographic hashing algorithm SHA-512 and each password is concatenated with unique salt value and hashed and stored. Salt Value and password hashes are stored in different tables in the database.

Guidance for Customers/Integrators:

- Customers are instructed to host the payment application in the PCI-DSS Compliant environment and for the data security in transit, TLS certificate must be installed in the web server and application should be accessed only through the HTTPS Protocol.
- Accessing the payment application through the web browser using Http protocol may result in data compromise and non-compliance to PCI-DSS standard

3.4

(Aligns with PCI DSS Requirement 7)

Limit access to required functions/resources and enforce least privilege for built-in accounts of payment application.

The payment application's application/service accounts by default have access,

- *Only to the function/resources for which it has specific purposes and*
- *At least privilege assigned for each function/resource as needed for the application/service account.*

Software Vendor Conformance:

EPay Advantage by default creates the user account only with the least privileges. Application / Service accounts has access only to the identified functions/resource which is required for the functioning of application

Guidance for Customers/Integrators:

Customers and application administrators are instructed to provide privilege to the ePay Advantage users only to the specific functions / modules of application upon business requirement and based on their job role to execute such functions. For the payment application account, provide access only to the specific identified user account for a particular location (Directory path) or resources access (Servers) for which they are intended so.

4 Log payment application activity

4.1

(Aligns with PCI DSS Requirement 10.1)

At the completion of the installation process, the "out of the box" default installation of the payment application must log all user access and be able to link all activities to individual users

The Payment application should,

- *Enable audit trails automatically upon installation*

Software Vendor Conformance:

EPay Advantage by default enables the audit trails upon the completion of installation. By default audit trails are stored in the database. Access to the audit log files is restricted only to the System / Application administrator. Access to the audit trail in the database should also be restricted and access to the audit logs should also be logged.

No other application users have access to the audit logs. Audit log configuration access is available only to the application administrator and by default audit log contains fields such as Date & Time, Affected entities/user, User identification, type of event, Success or failure indication, origination of event, Source IP Address.

Changing the default audit log contents is neither available for administrators nor to the normal users of application.

Guidance for Customers/Integrators:

Customer should never disable, or edit the audit trail and doing so will result in non-compliance with PCI DSS.

4.2 & 4.3

(Aligns with PCI DSS Requirement 10.2 & 10.3)

Payment application must provide automated audit trails to reconstruct the following events:

- *PA-DSS 4.2.1: All individual user accesses to cardholder data from the application*
- *PA-DSS 4.2.2: All actions taken by any individual with administrative privileges as assigned in the application*
- *PA-DSS 4.2.3: Access to application audit trails managed by or within the application*
- *PA-DSS 4.2.4: Invalid logical access attempts*
- *PA-DSS 4.2.5: Use of, and changes to the application's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.), and all changes, additions, deletions to application accounts with root or administrative privileges*
- *PA-DSS 4.2.6: Initialization, stopping, or pausing of the application audit logs*
- *PA-DSS 4.2.7: Creation and deletion of system-level objects within or by the application*

Payment application must record at least the following audit trail entries for each event,

- *PA-DSS 4.3.1: User identification*
- *PA-DSS 4.3.2: Type of event*
- *PA-DSS 4.3.3: Date and time*
- *PA-DSS 4.3.4: Success or failure indication*
- *PA-DSS 4.3.5: Origination of event*
- *PA-DSS 4.3.6: Identity or name of affected data, system component, or resource*

Software Vendor Conformance:

The ePay Advantage application, logs the following events

- All individual user access to cardholder data
- Actions taken by any individual with administrative privileges
- All access to the database where the cardholder data is stored
- Access to audit trails
- Invalid logical access attempts
- All actions taken for identification and authentication including user login, failed login attempts, creation of new users and deletion of users is logged
- Initialization, stopping, or pausing of the application audit logs
- Creation and deletion of system-level objects within or by the application
- Audit trail by default contains the information such as User Identification, Date & Time, Source IP Address, Type of Event, Success or failure, Source or Origination of Event, Affected user or data or components for every application events.

Operating Environment Logging

- Audit policy / Audit Trail should be enabled in the operating system to log all the administrative activities performed in the OS level
- Event logging must be enabled and all the changes to the operating system's identification and authentication mechanisms (including but not limited to creation of new accounts, elevation of privileges, etc.), and all changes, additions, deletions or modifications to operating systems critical files with root or administrative privileges must be logged and logs should be backed up to a Centralized logging server as per PCI-DSS Requirement 10.5.3

Guidance for Customers/Integrators:

Customer should never disable the audit trail and doing so will result in non-compliance with PCI DSS standard. It's the responsibility of the customer to maintain the PCI-DSS compliant environment and logging par with PCI-DSS Requirement 10.2

4.4

(Aligns with PCI DSS Requirement 10.5.3)

Payment application must facilitate centralized logging

Software Vendor Conformance:

EPay Advantage facilitates centralized logging into the Microsoft SQL Server database. Logging information can be obtained from the ePay database table [aspnet_WebEvent_Events]. Using the below command in a SQL query against the ePay database will return the logging data from the ePay database. This data can then be migrated to a centralized logging environment.

```
SELECT * FROM [aspnet_WebEvent_Events]
```

Guidance for Customers/Integrators:

EPay Advantage by default stores the audit log in the database. Customer are instructed to follow the above mentioned steps to send the payment application logs to the centralized logging server

5 Develop Secure Payment Applications

5.1

(Aligns with PCI DSS Requirement 6.3)

Developing payment applications in accordance with PCI DSS and PA-DSS Requirements

Software Vendor Conformance:

EPay Advantage is developed in accordance with PCI DSS and PA-DSS standards and Software Development processes are based on industry standards and best practices.

Security reviews are performed on regular basis prior to release of an application or application update.

PA-DSS Requirement 5.1 through 5.1.7 are the information related to the Software Development Processes are excluded from this guide.

5.2

(Aligns with PCI DSS Requirement 6.5)

Develop all payment applications to prevent common coding vulnerabilities in software-development processes

Software Vendor Conformance:

EPay Advantage is tested against the vulnerabilities listed in PA-DSS Requirements 5.2.1 through 5.2.10 and in PCI DSS at 6.5.1 through 6.5.10 and with Industry standards such as OWASP Top 10, SANS CWE Top 25. All the identified vulnerabilities are mitigated prior to the release of an application or application update. The latest industry trusted tools & techniques to identify and mitigate known vulnerabilities before the application release.

5.3

(Aligns with PCI DSS Requirement 6.4.5)

Software vendor must follow change-control procedures for all application changes. Change-control procedures must follow the same software development processes as new releases defined in PA-DSS Requirement 5.1

Software Vendor Conformance:

EPay Advantage changes are followed through proper change control mechanism. Any bug or feature enhancements reported by the customers introduce change in the application. For every application changes, Change Request document will be created with unique id allotted for each change. Each Change Request document records the Change request information, Documentation of impact, Functionality Test details, Installation and Back-out procedures, and Test results of change in the test environment before moving the change to production and approval of change by authorized parties.

Changes are deployed to the production environment post approval of authorities and successful testing.

5.4

Payment application vendor must document and follow a software-versioning methodology as part of their system development lifecycle. Versioning methodology must follow the procedures in the PA-DSS Program Guide for changes to payment applications

Software Vendor Conformance:

EPay Advantage application versioning methodology follows the procedures mentioned in PA-DSS Program guide. Application Release Notes will contain the changes incorporated in the specific version of application release, security impact and how the changes will affect the product version. The Release Notes will be published along with the application release and will be communicated to the customers.

EPay Advantage versioning uses the following four value methodology. (Example 6.0.1.002).

- The first digit refers to a major core release for basic application functionality. This level of change would have an impact to security functionality and PA-DSS requirements
- The second digit refers to minor feature set release that would add additional features while having no impact to security or PA-DSS requirements
- The third digit refers to a service pack release that will be used to address known issues and have little to no impact on the application functionality.
- The fourth digit identifies the internal maintenance version assigned by the development team.

Guidance for Customers/Integrators:

Application versioning methodology will be included in the PA-DSS implementation guide, where customers should read and understand the versioning methodology which will help them to find out payment application versions in use is PA-DSS Validated Version.

Customer can check the PA-DSS Application validation status in the PCI Council Website, under the Section List of Validated Payment Application to ensure the version of application in use is PA-DSS Certified

5.5 & 5.6

Usage of Risk Assessment Techniques during the Software Development Process and process of documenting and authorizing the final release of application

Software Vendor Conformance:

The above requirement 5.5 & 5.6 belongs to the Software Development Processes and it has been taken care during the development and Release phases. Hence detailed information on this requirement is excluded from the guide.

6 Protect Wireless Transmissions

Payment applications using wireless technology, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. The wireless technology must be implemented securely.

Software Vendor Conformance:

EPay Advantage is not developed for use with wireless technology and hence this requirement is not applicable.

Guidance for Customers/Integrators:

EPay Advantage is not developed and does not support for use with wireless technology. If wireless technology is used only to access the ePay Advantage, ensure that the below controls are in place.

Use of secure wireless connection in the client infrastructure (Must be followed if Wireless communication is in use)

- It is required to use a firewall between any wireless network and the LAN. (PCI DSS 1.2.3)
- The firewall must deny or control traffic from the wireless environment into the cardholder data environment. (PCI DSS 1.2.3)
- 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. (PCI DSS 4.1.1)
- Encryption keys were changed from default at installation (PCI DSS 2.1.1)
- Encryption keys must be changed anytime anyone with knowledge of the keys leaves the company or changes positions. (PCI DSS 2.2.1)
- Default SNMP community strings on wireless devices were changed. (PCI DSS 2.1.1 b)
- Default passwords/passphrases on access points were changed. (PCI DSS 2.1.1 b)
- Firmware on wireless devices is updated to support strong encryption for authentication (PCI DSS 2.1.1 d)

Note: It is prohibited to use WEP encryption mechanism

6.2

(Aligns with PCI DSS Requirement 4.1.1)

For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Software Vendor Conformance:

EPay Advantage is not developed for use with wireless technology and hence this requirement is not applicable

6.3

(Aligns with PCI DSS Requirement 1.2.3, 2.1.1, & 4.1.1)

Provide instructions for customers about secure use of wireless technology

Software Vendor Conformance:

EPay Advantage is not developed for use with wireless technology. However PCI DSS-compliant wireless settings should be configured if the wireless communication is used in the internal network.

Guidance for Customers/Integrators:

Customers must ensure the secure configuration of wireless network in their environment. Below are the minimum security controls to be in place if wireless network is used internally.

- Change default Wireless Administrator Username and Password
- Change all wireless default encryption keys, passwords, and SNMP community strings upon installation
- Change wireless encryption keys, passwords, and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions
- Install a firewall between any wireless networks and systems that store cardholder data and to configure firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- Use industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

7 Test payment applications to address vulnerabilities and maintain payment application updates

7.1

(Aligns with PCI DSS Requirement 6.1)

Software vendors must establish a process to identify and manage vulnerabilities

Software Vendor Conformance:

EPay Advantage development and Support team has subscribed to reputable sources such as NIST, NVD, US-CERT, Secunia for obtaining security vulnerability information related to the payment application. EPay Advantage is tested for the presence of vulnerabilities prior to release

Guidance for Customers/Integrators:

Customer are instructed to subscribe to the reputable sources such as NIST, NVD, US-CERT, Secunia, Vendor guidelines for obtaining security vulnerability information related to the application's infrastructure (Operating Systems and System applications).

Customer should regularly update the security patches of Operating System / Application

(Eg: IIS Web Server, Web Browser, Microsoft SQL Server and associated plug-ins required for the secure functioning of payment application) after proper testing

7.2 & 7.3

Software vendors must establish a process for timely development and deployment of security patches and upgrades and must include release notes for all application updates

Software Vendor Conformance:

Once the payment application related vulnerabilities have been identified, development team will work on releasing the patch/fix to customers. As Nodus tracks which versions of ePay has been deployed to the customer's environment, customers on the effected version will be notified of the issue and a patch will be delivered to resolve the issue. Within the patch package, notes pertaining to the changes made will be included as well as instructions for secure deployment of the updated files. The customer will be asked to confirm the version number of ePay has been updated after the patch has been deployed.

Guidance for Customers/Integrators:

Customers are instructed to follow the instructions provided with the patch for the secure patch deployment

8 Facilitate secure network implementation

8.1

(Aligns with PCI DSS Requirement 1,3,4,5 and 6)

Payment Application must not interfere with use of devices, applications, or configurations required for PCI DSS compliance.

Eg: Payment application cannot interfere with installation of patches, anti-malware protection, firewall configurations, or any other device, application, or configuration required for PCI DSS compliance

Software Vendor Conformance:

EPay Advantage does not interfere with the use of any device, application or configuration required to maintain PCI DSS Compliance

Guidance for Customers/Integrators:

Not Applicable

8.2

(Aligns with PCI DSS Requirement 2.2.2)

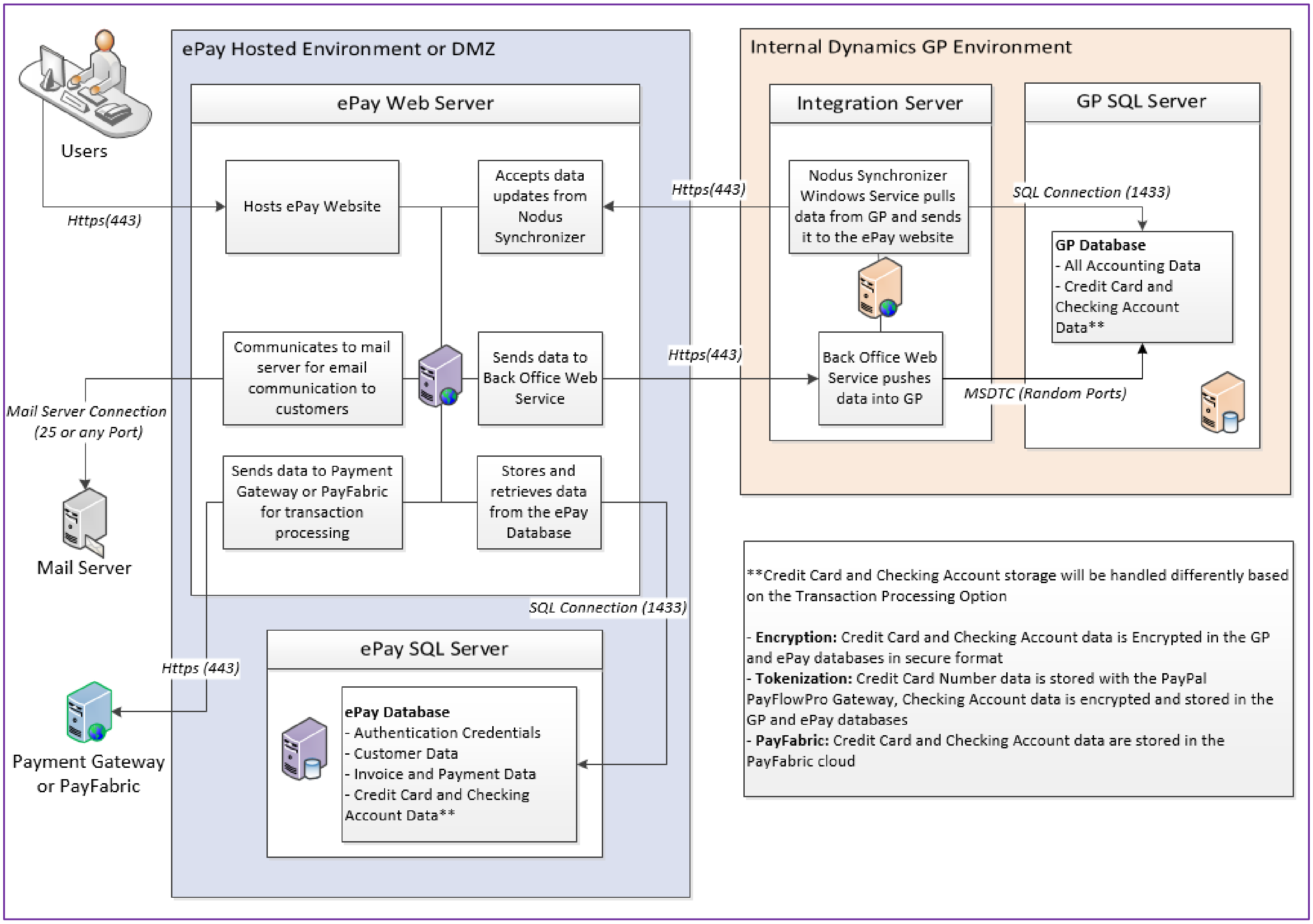
The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application.

Software Vendor Conformance:

EPay Advantage by default uses and enables only the services, protocols, ports, daemons, component, dependent software and hardware which are required for the proper functioning of payment application. All the services, ports, protocols which are not required for the payment application to be disabled by the system administrators.

List of services, ports, protocols used by ePay Advantage

Description	Port
User access to ePay	ePay Web Server - 443 Inbound
ePay to communicate the payment gateway or PayFabric	ePay Web Server - 443 Outbound
SQL Connection to ePay database	ePay Web Server – 1433 Outbound* ePay SQL Server – 1433 Inbound* (1433 is configured by SQL by default, but it may be modified by the database administrator)
ePay to communicate to a mail server	ePay Web Server – Mail Server port outbound
ePay to communicate to the Integration server web service	ePay Web Server - 443 Outbound Integration Server – 443 Inbound
Integration server to communicate to ePay web service	ePay Web Server – 443 Inbound Integration Server – 443 Outbound
Integration Server to communicate to the GP database	Integration server must have no blocked ports to GP SQL Server to utilize MSDTC protocol


Users
Https(443)
ePay Hosted Environment or DMZ
ePay Web Server
Hosts ePay Website
Accepts data updates from Nodus Synchronizer
Communicates to mail server for email communication to customers
Sends data to Back Office Web Service
Sends data to Payment Gateway or PayFabric for transaction processing
Stores and retrieves data from the ePay Database
Mail Server Connection (25 or any Port)
Mail Server
Https (443)
Payment Gateway or PayFabric
SQL Connection (1433)
ePay SQL Server
ePay Database
- Authentication Credentials
- Customer Data
- Invoice and Payment Data
- Credit Card and Checking Account Data**
Https(443)
Https(443)
Internal Dynamics GP Environment
Integration Server
Nodus Synchronizer Windows Service pulls data from GP and sends it to the ePay website
Back Office Web Service pushes data into GP
GP SQL Server
SQL Connection (1433)
GP Database
- All Accounting Data
- Credit Card and Checking Account Data**
MSDTC (Random Ports)

**Credit Card and Checking Account storage will be handled differently based on the Transaction Processing Option

- **Encryption:** Credit Card and Checking Account data is Encrypted in the GP and ePay databases in secure format
- **Tokenization:** Credit Card Number data is stored with the PayPal PayFlowPro Gateway, Checking Account data is encrypted and stored in the GP and ePay databases
- **PayFabric:** Credit Card and Checking Account data are stored in the PayFabric cloud

Guidance for Customers/Integrators:

Customer should harden the servers and applications as per the vendor security guidelines and run only the services, ports and protocols which are required for the application mentioned above. All the unwanted services to be disabled.

8.3

(Aligns with PCI DSS Requirement 8.3)

Payment application must not interfere with normal operation of multi-factor authentication technologies for secure remote access (network-level access originating from outside the network) to network resources residing within the CDE).

Software Vendor Conformance:

EPay Advantage does not interfere with the use of multi-factor authentication used for securing remote access originating from outside of CDE towards network resources residing within the CDE. EPay Advantage does not support a remote access mechanism.

Guidance for Customers/Integrators:

Not Applicable

9 Cardholder data must never be stored on a server connected to the Internet

9.1

(Aligns with PCI DSS Requirement 1.3.7)

The payment application must be developed such that any web server and any cardholder data storage component (for example, a database server) are not required to be on the same server, nor is the data storage component required to be on the same network zone (such as a DMZ) with the web server

Software Vendor Conformance:

EPay Advantage supports deployment in a 3-Tier architecture (Web Server/Integration Server/Database Server). It does not requires the server which stores cardholder data to be in the DMZ or on the same network zone.

Guidance for Customers/Integrators:

- Do not store cardholder data on public-facing systems (for example, web server and database server must not be on same server or same network segment)
- Refer the deployment architecture diagram for the payment application configuration
- Refer Sec PA-DSS 8.2 for the list of services/ports that application requires to communicate between two network zones

10 Facilitate secure remote access to payment application

10.1

(Aligns with PCI DSS Requirement 8.3)

Multi-factor authentication must be used for all remote access to the payment application that originates from outside the customer environment

Software Vendor Conformance:

EPay Advantage does not provide the functionality for remote access. Hence this requirement is not applicable. Any remote access to the server at the operating system layer must require the organization implementing a multi-factor authentication mechanism if access to the payment application server is originating from outside the customer environment to access the server.

Guidance for Customers/Integrators:

All remote access originating from outside the customer's network to the payment application servers must use multi-factor authentication in order to meet PCI DSS requirements.

10.2

(Aligns with PCI DSS Requirement 1 and 12.3.9)

Any remote access into the payment application must be performed in secure manner

Software Vendor Conformance:

EPay Advantage does not employ any remote access mechanism to support services remotely or to provide remote payment application updates. There is no automatic update process that identifies and downloads application updates available for ePay Advantage via remote access technologies. Hence this requirement is not applicable

Guidance for Customers/Integrators:

Not applicable

11 Encrypt sensitive traffic over public networks

11.1

(Aligns with PCI DSS Requirement 4.1)

If the payment application sends, or facilitates sending, cardholder data over public networks, the payment application must support use of strong cryptography and security protocols (for example, TLS/TLSIPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks

Software Vendor Conformance:

EPay Advantage uses secure HTTPS protocol for the communication across all open and public networks. Even for the internal access of the payment application in the intranet we implement and recommend the use of self-signed TLSv1.2 certificates for the secure access of payment application.

Guidance for Customers/Integrators:

Customers are instructed to,

- Install the CA issued TLSv1.2 certificates and access payment application only via HTTPS protocol
- Kindly follow the ePay Installation Guide to securely configure the payment application
- Verify that HTTPS appears as a part of the browser Universal Record Locator (URL)
- Verify that only trusted TLS keys/certificates are accepted
- Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)

11.2

(Aligns with PCI DSS Requirement 4.2)

If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs

Software Vendor Conformance:

EPay Advantage does not facilitate sending of PANs by end-user messaging technologies, hence this requirement is not applicable. EPay Advantage with the Encryption Option enabled, all the PAN's are encrypted and stored in the database and masked in reports when it is displayed. The full PAN number is not visible from ePay Advantage.

Guidance for Customers/Integrators:

Customers are instructed not to use any end-user messaging technologies for sending the PAN numbers in the internal or external network. The payment application administrator at the customer environment is responsible for providing access on the role based for the users of payment application

12 Secure all non-console administrative access

12.1 & 12.2

(Aligns with PCI DSS Requirements 2.3 and 8.3)

All non-console administrative access must be encrypted with strong cryptography technologies such as SSH, VPN, or TLS, for web-based management and other non-console administrative access.

Use multi-factor authentication for all personnel with non-console administrative access.

Software Vendor Conformance:

Administrative access to the Web, App and database servers are possible through non-console access. In case, if non-console administrative access is used for accessing any of the servers that belongs to CDE environment, the session must be always encrypted using TLS, SSH or VPN

As card data is not available through non-console administrative access therefore requirement 12.2 is not applicable.

Guidance for Customers/Integrators:

- All non-console administrative access should be secured using technologies such as SSH, VPN, or TLS, for web-based management and other non-console administrative access
- Note: Clear-text protocols such as Telnet or rlogin must never be used for administrative access. SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

12.2

(Aligns with PCI DSS Requirement 8.3)

Use multi-factor authentication for all personnel with non-console administrative access.

Software Vendor Conformance:

EPay Advantage does not utilize or restrict multi-factor authentication methods to access the servers with administrative access.

Guidance for Customers/Integrators:

- All non-console administrative access should be secured using technologies such as SSH, VPN, or TLS, for web-based management and other non-console administrative access
- Note: Clear-text protocols such as Telnet or rlogin must never be used for administrative access. SSL and early TLS are not considered strong cryptography. Payment applications must not use, or support the use of, SSL or early TLS. Applications that use or support TLS must not allow fallback to SSL.

13 Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators

13.1

Develop, maintain, and disseminate a PA-DSS Implementation Guide(s) for customers, resellers, and integrators

Software Vendor Conformance:

This guide addresses the PA-DSS Requirement 13. The ePay PA-DSS Implementation guide will be provided to the customer along with the payment application, which will help the customer/ integrators to securely configure the payment application as mentioned in the ePay PA-DSS Implementation guide. Updates to PA-DSS Implementation guide will be communicated to the customer and updated version of the Implementation guide will be provided.

Guidance for Customers/Integrators:

- The customer must go through the PA-DSS Implementation guide and host the application as mentioned in the document
- The customer is responsible for ensuring secure deployment of PA-DSS application in the PCI-DSS certified environment
- PA-DSS Implementation Guide will be reviewed and revised upon
    - At least annually
    - Upon changes to the application
    - Upon changes to the PA-DSS requirements

EPay Advantage - End User License Agreement (EULA)

Important – Read Carefully. This Nodus End-User License Agreement ("Agreement") is a legal agreement between you ("End-User") (on the one hand) and Nodus Technologies, Inc. ("Nodus") and its OEM partner(s) ("OEM") (on the other hand), for the software product identified above, which includes computer software and may include associated media, printed materials, and online or electronic documentation (the "Product"). By installing, copying, other otherwise using this Product, you agree to be bound by the terms of this Agreement. If you, the End-User, do not agree to the terms of this Agreement, do not install or use this Product; you may, however, return it to your place of purchase for a refund or credit.

This license is not a sale. Title and copyrights to the Product remain with Nodus and its OEM partner(s). Unauthorized copying of the data, or failure to comply with the provisions of this License Agreement, will result in automatic termination of this license and Nodus and its OEM partner(s) may use any other legal remedies available to it. IN THE EVENT OF LICENSE TERMINATION, ALL MATERIALS, DATABASES, AND DOCUMENTATION MUST BE IMMEDIATELY RETURNED TO NODUS TECHNOLOGIES, INC. AT THE ADDRESS LISTED AT THE END OF THIS AGREEMENT.

1. End-User represents and warrants that it is authorized and empowered to enter into this Agreement. Nodus represents and warrants that it is authorized and empowered to grant the rights hereinafter set forth.

2. Nodus and its OEM Partner(s) hereby grant End-User a non-exclusive, non-transferable right to use the Product, subject to the use restrictions and limitations set forth below.

3. Nodus shall provide End-User with one (1) machine-readable copy of the Product. This license authorizes use of the Product at a single location, which shall mean a single location which uses or accesses the Product either from a computer or terminal on site or through a computer or terminal at a supporting location.

4. End-User acknowledges that the Product is confidential, proprietary material owned and copyrighted by Nodus. End-User agrees that Nodus and its OEM partner(s) shall retain exclusive ownership of the Product, including all literary property rights, patents, copyrights, trademarks, trade secrets, trade names, or service marks, including goodwill and that Nodus may enforce such rights directly against End-User in the event the terms of this Agreement are violated.

5. The Product is intended for use solely by End-User for their own internal purposes as an alternative electronic information source of data. The Product may only be used at the location(s) licensed and paid for by End-User to the Nodus. End-User agrees not to copy, modify, sub-license, assign, transfer or resell the Product, in whole or in part. End-User agrees not to translate, reverse engineer, decompile, disassemble, or make any attempt to discover the source code of the Product (except and only to the extent applicable law prohibits such restrictions). End-User further agrees not to download/upload the Product, in whole or in part, or to establish a network, place data on the Internet or otherwise publish, or offer a service bureau utilizing the Product. End-User agrees to restrict access to the Product to designated employees and to use its best efforts to prevent violation of these restrictions by agents, employees and others, taking such steps and reasonable security precautions as may be necessary. End-User shall permit Nodus and/or its representative access to its premises during normal business hours to verify compliance with the provisions of this Agreement.

6. Without prejudice to any other rights, Nodus may terminate this Agreement if End-User does not abide by the terms and conditions of this Agreement. Upon termination of this Agreement, all licenses and rights to use the Product shall immediately terminate and End-User shall immediately cease any and all use of the Product. Within thirty (30) days after termination of the Agreement, End-User shall return to Nodus, postage prepaid, all copies of the Product.

In the event that the End-User fails to pay the periodic maintenance fee, unless such periodic maintenance fee is waived in writing by Nodus, then Nodus shall no longer be obligated to provide any services or support to End-User nor shall Nodus be obligated to provide any additional upgrades or updates for such Product or any other service or Product. Nodus reserves the right to discontinue any services provided to End-User or made available to End-User through the use of the Product.

7. All UPDATES provided by Nodus and its affiliates shall be considered part of the Product and subject to the terms and conditions of this Agreement. Additional license terms may accompany UPDATES. By installing, copying, or otherwise using any UPDATE, End-User agrees to be bound by this Agreement and any terms accompanying each such UPDATE. If End-User does not agree to the additional license terms accompanying such UPDATES, do not install, copy, or otherwise use such UPDATES.

8. End-User agrees that Nodus and its affiliates may collect and use information End-User provides as a part of support services, problem resolution or technical improvements or developments in connection with the Product.

9. End-User acknowledges that the Product is of U.S. origin and agrees to comply with all applicable international and national laws that apply to the Product, including the U.S. Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments.

10. NODUS REPRESENTS THAT THE PRODUCT DOES NOT VIOLATE OR INFRINGE ANY PATENT, TRADEMARK, TRADE SECRET, COPYRIGHT, OR SIMILAR RIGHT. IN THE EVENT THE PRODUCT IS HELD TO INFRINGE THE RIGHTS OF ANY THIRD PARTY, NODUS SHALL HAVE THE OPTION EITHER TO PROCURE THE RIGHT FOR THE END-USER TO CONTINUE USING THE PRODUCT OR AT NODUS'S EXPENSE, TO REPLACE OR MODIFY THE PRODUCT SO THAT IT BECOMES NON-INFRINGING. NODUS AND ITS OEM PARTNER(S) MAKE NO OTHER WARRANTY, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE ACCURACY OF THE PRODUCT OR THE MERCHANTABILITY AND FITNESS OF THE PRODUCT FOR A PARTICULAR PURPOSE. FURTHER, NODUS DOES NOT WARRANT THE COMPATIBILITY OF THE PRODUCT WITH END-USER'S COMPUTER HARDWARE AND/OR SOFTWARE SYSTEM.

11. End-User's sole and exclusive remedy for any damage or loss in any way connected with the Product furnished herein, whether by breach of warranty, negligence, or any breach of any other duty, shall be, at Nodus' option, replacement of the Product or return or credit of an appropriate portion of any payment made by End-User with respect to such Product. Under no circumstances shall Nodus or its OEM Partner(s) be liable to End-User or any other person for any indirect, incidental, special or consequential damages of any kind, however, caused and regardless of theory of liability, including, without limitation, for lost profits, loss of data, loss of goodwill, business interruption, computer failure or malfunction or any and all other commercial damages or losses. This limitation will apply even if Nodus has been advised of the possibility of such damage. Some jurisdictions do not allow the exclusion of a limitation of indirect, incidental, special or consequential damages, so the above exclusion may not apply to such End-Users. In such event, Nodus' total liability to End-User for all damages shall be limited to the amount of fifty dollars ($50.00).

12. Nodus may cancel this license at any time if End-User fails to comply with the terms and conditions of this Agreement; and Nodus may obtain injunctive relief and may enforce any other rights and remedies to which it may be entitled in order to protect and preserve its proprietary rights.

13. This Agreement is the complete and exclusive statement of the understanding between the parties, with respect to the subject matter, superseding all other agreements, representations, communications, advertisements, statements and proposals, oral or written.

14. No term or provision hereof shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or

waiver of, a breach by the other, whether express or implied, shall not constitute a consent to, waiver of, or excuse for any other different or subsequent breach.

General

The internal laws of the State of California shall govern this Agreement. If any provision of the Agreement is held invalid, the remainder of the Agreement shall continue in full force and effect. If you have any questions, please contact in writing: Nodus Technologies, Inc., 2099 S. State College Blvd., Suite 250, Anaheim, CA 92806, Tel: (909) 482-4701

Copyright Information

The names of companies, products, people, and/or data used in window illustrations and sample output are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

Warranty Disclaimer Nodus technologies, Inc. disclaim any warranty regarding the sample code contained in this documentation, including the warranties of merchantability and fitness for a particular purpose.

Limitation of Liability The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Nodus Technologies, Inc. Nodus Technologies, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual. Neither Nodus Technologies, Inc. nor anyone else who has been involved in the creation, production or delivery of this documentation shall be liable for any indirect, incidental, special, exemplary or consequential damages, including but not limited to any loss of anticipated profit or benefits, resulting from the use of this documentation or sample code.

License agreement Use of this product is covered by a license agreement provided with the software product. If you have any questions, please call Nodus Technologies Support at 909-482-4701