Distribution iBusiness (A+) - Electronic Payments v08.03
PA-DSS 2.0 Implementation Guide

Version 1.0

January 2012

Confidential Information

Table of Contents

Notice 3

About this Document....4

Legal Terms and Conditions 5

Revision Information 6

Executive Summary 7

Application Summary 7

Typical Network Implementation 10

Distribution iBusiness (A+) Network Diagram Example 10

Distribution iBusiness (A+) Authorization Data Flow Diagram 11

Difference between PCI Compliance and PA-DSS Validation 12

Considerations for the Implementation of Distribution iBusiness (A+) in a PCI-Compliant Environment....13

Remove Historical Sensitive Authentication Data (PA-DSS 1.1.4.a) 13

Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c) 13

Purging of Cardholder Data (PA-DSS 2.1) 14

Cardholder Data Encryption Key Management (PA-DSS 2.5.c and 2.6.a) 15

Removal of Cryptographic Material (PA-DSS 2.7.a)....17

Set up Strong Access Controls (3.1.a and 3.2) 17

Properly Train and Monitor Admin Personnel....20

Log settings must be compliant (PA-DSS 4.1.b, 4.4.b)....21

Services and Protocols (PA-DSS 5.4.c) 26

PCI-Compliant Wireless settings (PA-DSS 6.1.f and 6.2.b) 26

Never store Cardholder Data on internet-accessible systems (PA-DSS 9.1.b)....27

PCI-Compliant Remote Access (10.2) 27

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1) 27

PCI-Compliant Remote Access (10.3.2.b)....28

Data Transport Encryption (PA-DSS 11.1.b)....29

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2.b) 29

Non-console Administration (PA-DSS 12.1)....30

Network Segmentation....30

Maintain an Information Security Program 30

Application System Configuration....30

Payment Application Initial Setup & Configuration 31

Payment Application Software Update Setup & Configuration 32

Notice

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

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

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

About this Document

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

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

You must follow the steps outlined in this *Implementation Guide* in order for your Distribution iBusiness (A+) Electronic Payments installation to support your PCI DSS compliance efforts.

Legal Terms and Conditions

Acceptance of a given payment application by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (*the "Accepted Version"*). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and accepted by PCI SSC – even if the different payment application or version (*the "Alternate Version"*) conforms to the basic product description of the *Accepted Version* – then the *Alternate Version* should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.

No vendor or other third party may refer to a payment application as "*PCI Approved*" or "*PCI SSC Approved*", and no vendor or other third party may otherwise state or imply that PCI SSC has, in whole or part, accepted or approved any aspect of a vendor or its services or payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC's approval or acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC shall be provided by the party providing such products or services, and not by PCI SSC, or any payment brands.

Revision Information

Date of Update	Version	Summary of Changes
12/07/11	1.0	Initial update
03/29/12	1.0	Finalized version 1.0 document

NOTE: This PA-DSS Implementation Guide must be reviewed on a yearly basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. Infor will distribute the Implementation Guide to customers via the Infor Xtreme Support Portal documentation link.

Executive Summary

Distribution iBusiness (A+) Electronic Payments v08.03.01 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Coalfire Systems, Inc. 361 Centennial Parkway Suite 150 Louisville, CO 80027	Coalfire Systems, Inc. 150 Nickerson Street Suite 106 Seattle, WA 98109

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

PCI Security Standards Council Reference Documents

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

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

Application Summary

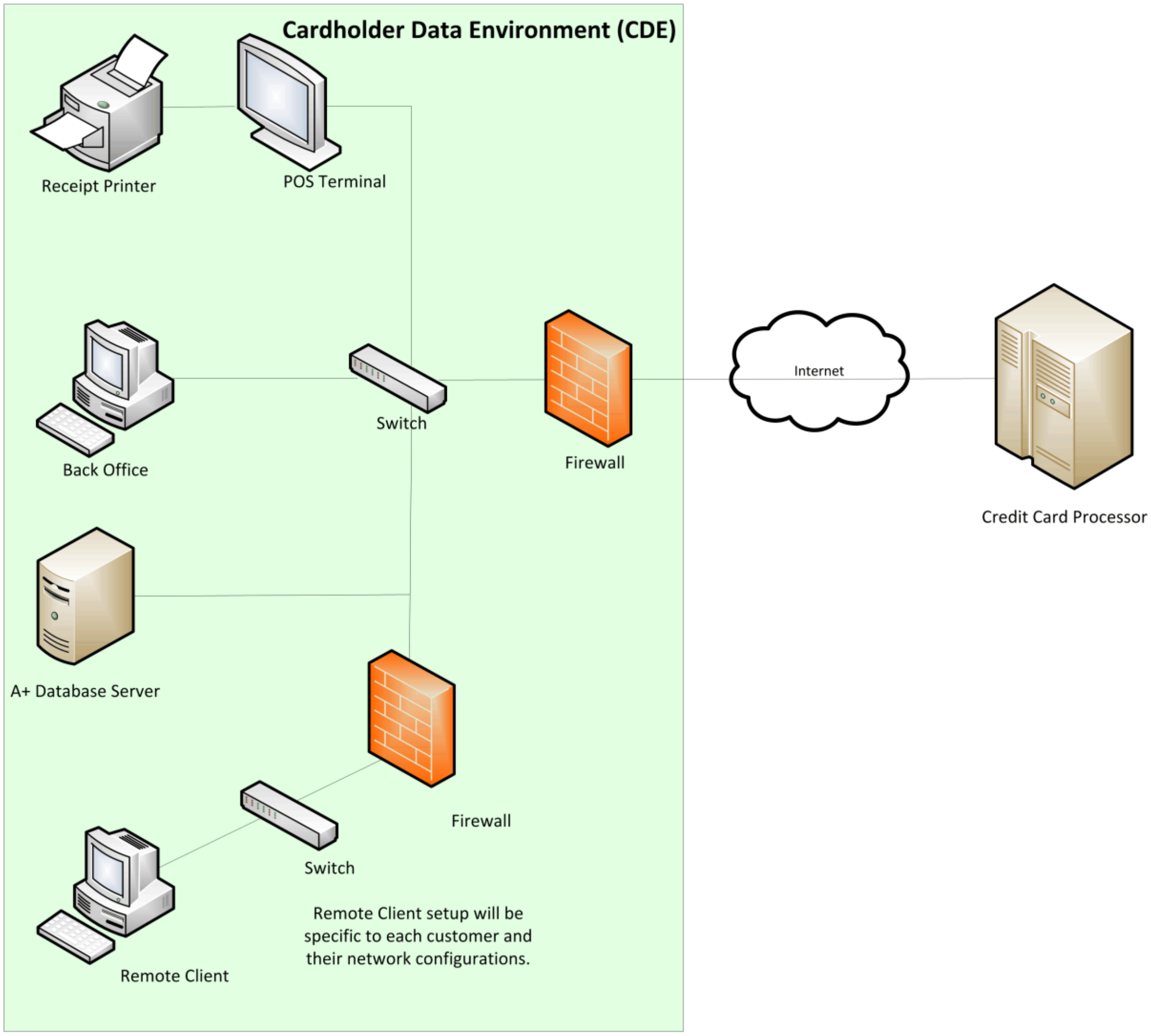
Payment Application Name:	Distribution iBusiness (A+) Electronic Payments
Payment Application Version:	v08.03.01
Application Description:	Electronic Payments provides seamless credit card integration with our proven Distribution iBusiness (A+) solution. With Electronic Payments, you can define multiple credit cards for your customers and authorize credit card payments through order entry, point of sale, and accounts receivable. All processing takes place in a totally secure environment, including encryption of cardholder data only within the database, and the masked display of only the last four digits of the primary account number on most screens and documents. Communications with authorization networks and payment service providers is enabled by full Distribution iBusiness (A+) integration with Payflow Pro by PayPal, Inc. or PAYware

	Transact by VeriFone Systems, Inc.
Application Target Clientele:	Distribution businesses, including Point of Sale functionality.
Components of Application Suite (i.e. POS, Back Office, etc.)	Distribution iBusiness (A+) base modules and Cross Applications installed at v08.03.01 or later installed on the IBM System i. Base modules include Accounts Receivable, Inventory Accounting, Order Entry, and Sales Analysis. Electronic Payments can optionally be used with Point of Sale, General Ledger, and International Currency modules. Based on the third party payment application, the TCP/IP Manager v1.03 (or higher) communications application is required for Payflow Pro by PayPal.
Required Third Party Payment Application Software:	Payflow Pro by PayPal, Inc. – Payflow Pro Software Development Kit for Windows Server 2003. -or- PAYware Transact by VeriFone Systems, Inc. – PAYware Transact v3.2.4
Database Software Supported:	DB2 for iSeries 8.1 (and newer) for i5/OS
Other Required Third Party Software:	None
Operating System(s) Supported:	IBM i 6.1 or later
Application Functionality Supported	Select one or more from the following list: □ **POS Suite** ☒ **POS Admin** □ **Shopping Cart & Store Front** ☒ **POS Face-To-Face** ☒ **Payment Middleware** □ **Others (Please Specify):** □ **POS Kiosk** ☒ **Payment Back Office** □ **POS Specialized** □ **Payment Gateway/Switch**
Payment Processing Connections:	Distribution iBusiness (A+) allows credit card payment processing to occur within three areas of the application including Order Entry, Point of Sale, and AR Quick Pay. Each area allows manual entry of credit card authorization information, while POS entry also allows for swipe card functionality. Once the credit card is keyed, read, or swiped, the cardholder data is sent from the station/unit PC to the credit card authorization server. At this point, the cardholder data is encrypted at this authorization server level utilizing secure communication methods (SSL/VPN), and is securely sent to the acquiring bank/payment service provider. When the authorization response is sent back, no track data or sensitive authentication

	data is stored in any database file, besides encrypted cardholder data. This unreadable cardholder data is primarily stored for Mail Order/Telephone Order (MOTO) processing and recurring billing purposes within Distribution iBusiness (A+).
Application Authentication:	Distribution iBusiness (A+) relies on the i7/OS authentication mechanism. Users must log into the OS level using PCI compliant credentials explained in this guide. The OS includes an "Initial Program to Load" in the user profile which defines the user's access to Distribution iBusiness (A+).
Description of Versioning Methodology:	Distribution iBusiness (A+) has three levels: VV.RR.SS VV = Version Usually Architecture changes (OS) and/or major DB changes to change Versions with fixes and enhancements RR = Release Database (DB) changes and larger enhancements with fixes SS = Service Packs Lower risk enhancements and fixes
List of Resellers/Integrators (If Applicable):	Maximum Computer Supply AKTion Associates

Typical Network Implementation

Distribution iBusiness (A+) Network Diagram Example

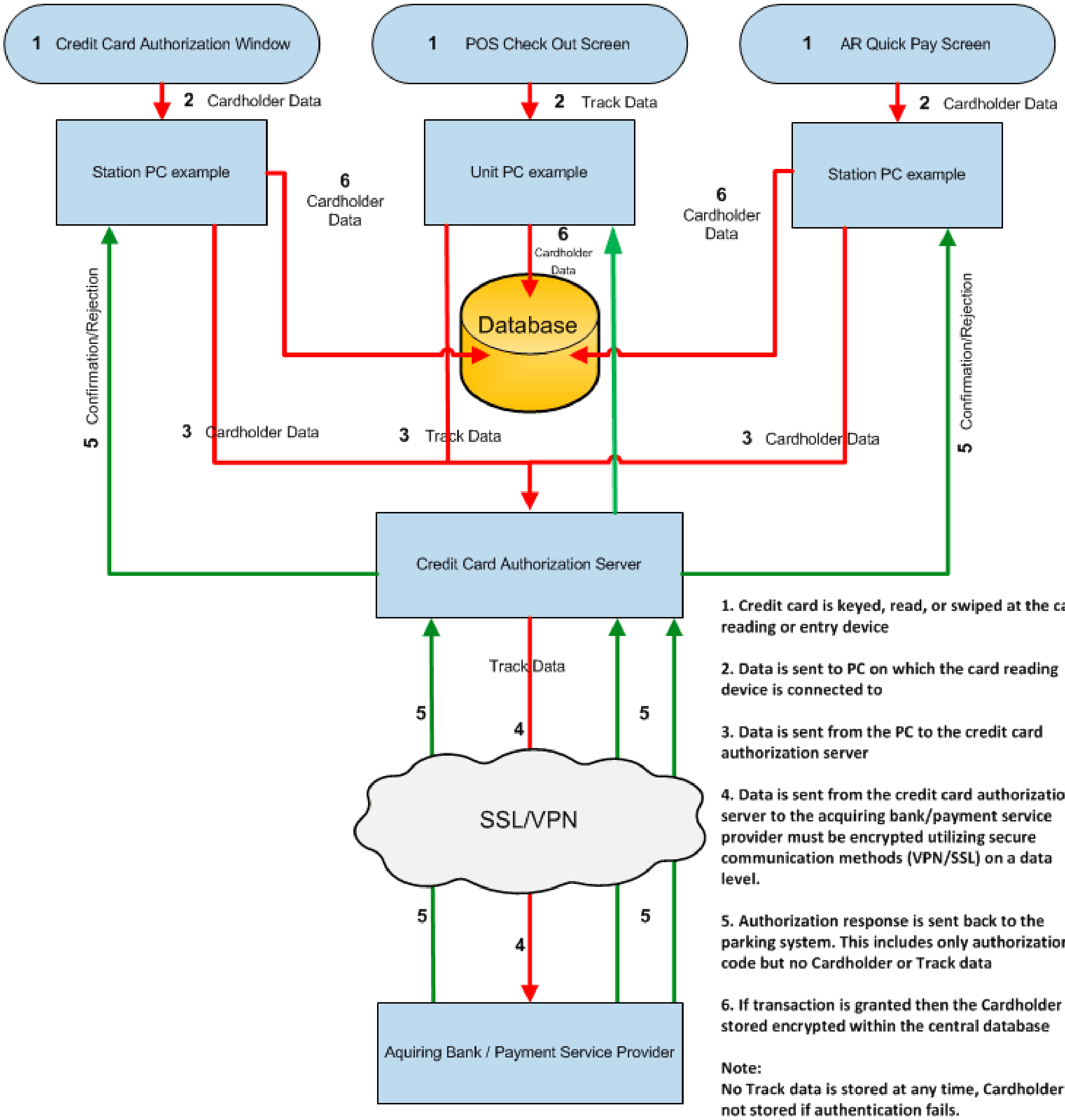


Remote Client setup will be specific to each customer and their network configurations.

Distribution iBusiness (A+) Authorization Data Flow Diagram

Distribution iBusiness (A+) Data Flow Diagram Example

Colored lines represent the type of data in transit as follows:
- Red represents encrypted or unencrypted Cardholder data in Transit
- Green represents data that is not considered Cardholder Data.



1. Credit card is keyed, read, or swiped at the card reading or entry device

2. Data is sent to PC on which the card reading device is connected to

3. Data is sent from the PC to the credit card authorization server

4. Data is sent from the credit card authorization server to the acquiring bank/payment service provider must be encrypted utilizing secure communication methods (VPN/SSL) on a data level.

5. Authorization response is sent back to the parking system. This includes only authorization code but no Cardholder or Track data

6. If transaction is granted then the Cardholder is stored encrypted within the central database

Note:
No Track data is stored at any time, Cardholder is not stored if authentication fails.

Difference between PCI Compliance and PA-DSS Validation

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

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

PA-DSS is the standard against which Distribution iBusiness (A+) has been tested, assessed, and validated.

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

Obtaining “PCI Compliance” is the responsibility of the merchant (distributor) and their hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that Distribution iBusiness (A+) will help the merchant (distributor) achieve and maintain PCI Compliance with respect to how Distribution iBusiness (A+) handles user accounts, passwords, encryption, and other payment data related information.

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

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

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

7. *Restrict access to data by business need-to-know*

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Considerations for the Implementation of Distribution iBusiness (A+) in a PCI-Compliant Environment

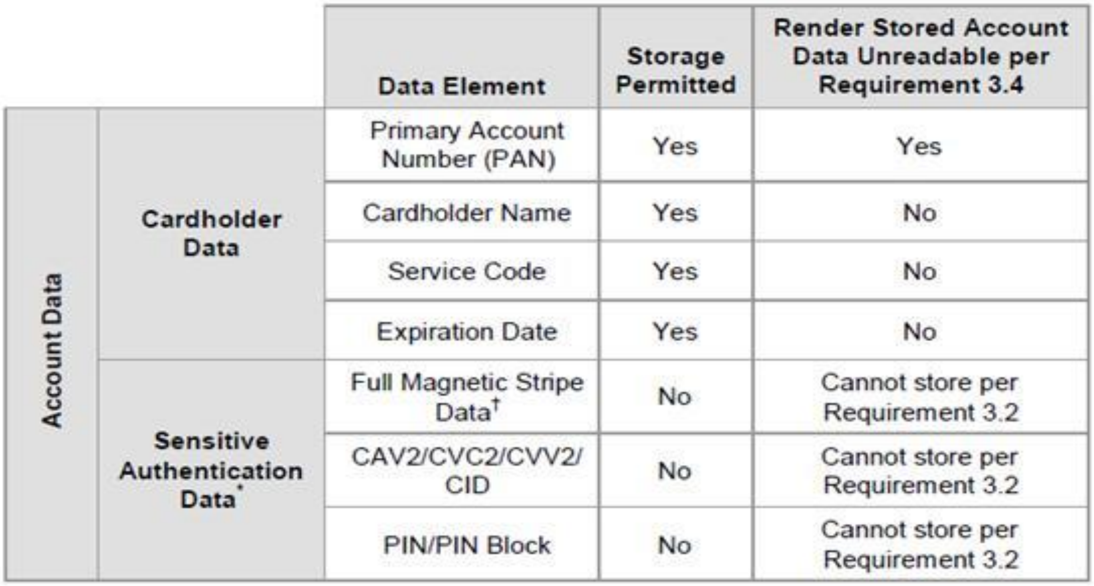
The following areas must be considered for proper implementation in a PCI-Compliant environment.

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

There are no legacy versions that ever stored sensitive authentication data such as the full magnetic stripe data, pin/pin block, or CAV2/CVC2/CVV2/CID. Therefore, there is no need for secure removal of such data.

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

Distribution iBusiness (A+) does not store any sensitive authentication data for any reason, and we recommend that you do not do so either. The table below indicates the difference between cardholder data and sensitive authentication data.



		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[*]	Full Magnetic Stripe Data[†]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

Only cardholder data storage of the primary account number (PAN), expiration date, and card holder name/address is encrypted and stored primarily for Mail Order/Telephone Order (MOTO) processing and recurring billing purposes within Distribution iBusiness (A+). However, if for any reason you do decide to store sensitive authentication data (stripe data, validation values or codes, PIN or PIN block data), the following guidelines must be followed:

- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

Purging of Cardholder Data (PA-DSS 2.1)

The Re-Encrypt Account Numbers functionality must be run on scheduled updates to both re-encrypt cardholder data and purge any cardholder data that is older than the number of days specified by the merchant (distributor) within this option. The retention period of cardholder data should be based on the policies and procedures specific to the merchant (distributor) with regard to the required number of days to save such data. As part of the merchant (distributor) implementation of Electronic Payments, a policy and procedure document should be created to identify business justifications for requirements pertaining to this retention period of cardholder data.

Distribution iBusiness (A+) includes the capability to securely and automatically *purge* cardholder data and *re-encrypt* existing cardholder data under the new advanced encryption methodology (AES 256 bit encryption). This re-encrypted cardholder data is to be stored in, and purged from, a new cardholder encryption file (introduced at version 08.01 of Distribution iBusiness (A+)).

In order for a customer to activate this advanced encryption and re-encrypt data under new keys, as well as purge existing cardholder data beyond the retention period, it is *mandatory* for the user to run the following option:

- Re-Encrypt Account Numbers (Menu EPFILE) - option 25

If the date of the cardholder data is older than the purge days specified, based on the defined retention period, this cardholder data will be completely deleted. However, if the date does not qualify for the cardholder data to be purged, this data will be securely re-encrypted.

Please understand the following important guidelines:

- To ensure inadvertent capture or retention of encrypted cardholder data, you should never journal any cardholder encrypted file in Distribution iBusiness (A+).

- The Customer Credit Card Account file will need to be purged *manually* by the merchant (distributor) based on their policies and procedures for keeping recurring billing and customer credit card information.

At version 08.03 of Distribution iBusiness (A+), the file attribute to '*Reuse Deleted Records*' has been changed from *NO to *YES. This means that newly added file records will overwrite previously deleted records within the file immediately, which provides a more efficient use of disk space. This would also mean that the space allocated for deleted records within each file will immediately be used for file writes and updates. This further ensures that past data is securely removed from disk whereby data is irretrievable.

Regardless if the current Distribution iBusiness (A+) version is at 08.03 or below, it should be a scheduled practice to perform the following processes in this order:

- Reorganize iBusiness (A+) History Files (Menu XAMAST) - option 18
    - This process allows you to purge individual history files by deleting records beyond a specified date.
- Remove Deleted Records from Files (Menu XAMAST) - option 23
    - This process requires Distribution iBusiness (A+) to be stopped, as it will physically remove deleted records from disk (reorganize space) in all files that reside in the file library.
    - The new cardholder encryption file containing unreadable cardholder data exists within the file library, further ensuring that purged encrypted data that existed in deleted record space is fully removed from disk.

NOTE – The above processes may be alternatively run as part of Day End Processing.

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

Cardholder data including the primary account number (PAN), expiration date, and card holder name/address is encrypted using an Advanced Encryption Standard (AES) 256 bit algorithm with key management capabilities.

The advanced encryption will randomly generate keys for each transaction and rely on native operations and APIs in the programming language (RPG) to encrypt data. Once the Data Encryption Keys (DEKs) have rendered the data unreadable, all data keys will also be encrypted under Key Encryption Keys (KEKs), which are stored encrypted in the key sequence encryption key database file. Further, KEKs are stored encrypted under the Master Key.

When advanced encryption is active (upon a mandatory run of the Re-Encrypt Account Numbers (MENU EPFILE) option), all cardholder data will be rendered unreadable and stored in the new database encryption file.

No action is required by the merchant for generation or storage of the encryption keys since these keys are generated randomly. Because keys will be stored securely under Key Encryption and Master Data Keys, all keys can be managed by system administrators. A merchant must define a crypto-period to which keys are replaced or retired. Cardholder data should be purged or re-encrypted under new keys at the end of each crypto-period or when the key is known or suspected to have been compromised or weakened. For Advanced Encryption Standard 256 algorithm, we recommend that your defined crypto-period not exceed two years.

Distribution iBusiness (A+) includes the capability to set up a Re-Encrypt Account Numbers Notification that will remind the merchant to re-encrypt under new keys near the end of the defined crypto-period.

The merchant can set up the Re-Encrypt Account Numbers Notification reminder within the following system option:

- Credit Card Options (Menu EPFILE) - option 1

This system option will display the date when the next Re-Encrypt Notification will be sent based on the number of days set by the merchant. The notification date is checked against today's date during the day end process and the reminder notification will be sent to the system operator message queue. If the Mail Server module is installed, along with Mail Gateway Express, the reminder notification will also be emailed to a distribution group defined by the merchant via Menu MSFILE options 4 & 5.

The following key management procedure must be performed by the merchant per PCI DSS:

- Run Re-Encrypt Account Numbers (MENU EPFILE) option 25. The following processes will occur automatically:
    - Generate strong cryptographic keys
    - Secure cryptographic key distribution
    - Secure cryptographic key storage
    - Cryptographic key changes for keys that reached the end of their crypto-period (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)
    - Retire keys when the integrity of the key has been weakened
    - Replace known or suspected compromised keys
    - If retired or replaced cryptographic keys are retained, the application cannot use these keys for encryption operations
- The following is *not applicable* to Distribution iBusiness (A+) because no manual clear-text key management is used. Keys are generated as dynamic keys.

    - Manual clear-text key-management procedures require split knowledge and dual control of keys
    - Prevention of unauthorized substitution of cryptographic keys

Removal of Cryptographic Material (PA-DSS 2.7.a)

Rendering previous cryptographic material irretrievable is absolutely necessary for you to remain PCI DSS compliant. Distribution iBusiness (A+) beginning with version 08.01 did encrypt and store cardholder data including the primary account number (PAN), expiration dates, and card holder names/addresses. That enhancement to the product brought us much closer to being compliant, however, was not fully compliant.

<u>Prior to version 08.03:</u>

- Customer must upgrade to version 08.03.01.
- Purge individual history files by deleting records beyond a specified date by running Reorganize iBusiness (A+) History Files (MENU XAMAST) option 18.
- Physically remove deleted records from disk (reorganize space) in all files that reside in the file library by running Remove Deleted Records from Files (MENU XAMAST) option 23.

<u>At version 08.03 and above:</u>

- Activate advanced encryption and re-encrypt data under new keys by running Re-Encrypt Account Numbers (MENU EPFILE) option 25. This process will also purge old encryption records (based on number of days specified), as well as replacing keys. *In accordance to industry-accepted standards, prior to physically removing/deleting these records from the file, the cryptographic materials will be overwritten with three different character sequences prior to deletion.*
- Purge individual history files by deleting records beyond a specified date by running Reorganize iBusiness (A+) History Files (MENU XAMAST) option 18.
- Physically remove deleted records from disk (reorganize space) in all files that reside in the file library by running Remove Deleted Records from Files (MENU XAMAST) option 23.
    - At version 08.03 and above, the file attribute to “Reuse Deleted Records” has been changed from *NO to *YES. This means that new file records will overwrite previously deleted records within the file, which provides a more efficient use of disk space. This would also mean that the space allocated for deleted records within each file will immediately be used for file writes and updates. This further ensures that past data is fully removed from disk whereby data is irretrievable.

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

The authentication credentials used by Distribution iBusiness (A+) during logon with a unique user ID and password is reliant on IBM System i level security and system values.

A further overview concerning details on security, sign-on, and passwords can be accessed via:

http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/index.jsp.

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 application.

In order to create strong authentication, the following points below must be followed:

System i Security Levels Set with the QSECURITY System Value

Security Level	Description
10	**No Passwords are Needed:** The system does not require a password to sign on. The user has access to all system resources. Security level 10 is not available unless your system is already running at this level. If you change from security level 10 to 20, 30, 40 or 50, you cannot change back to level 10.
20	**Password Security Only**: The system requires a password to sign on. Users have access to all system resources. Only a security officer or someone with security administrator (*SECADM) authority can create user profiles.
30	**Password and Object Security**: The system requires a password to sign on and users must have authority to access objects and system resources.
40 **[CERTIFIED]**	**Password, Object, and Operating System Integrity Security**: The system requires a password to sign on and users must have authority to access objects and system resources. Programs fail if they try to access objects through interfaces that are not supported.
50	**Password, Object, and Enhanced Operating System Integrity Security**: The system requires a password to sign on and users must have authority to access objects and system resources. Programs fail if they try to pass unsupported parameter values to supported interfaces or if they try to access objects through interfaces that are not supported.

1. The System i password must to be at least **7** characters.

System i Security Levels Set with the QPWDLVL System Value

Password Level	Description
0	User profile passwords with a length of 1 – 10 characters are supported.
1	User profile passwords with a length of 1 – 10 characters are supported. i5/OS NetServer passwords for Windows 95/98/ME clients will be removed from the system. Note: Windows 2000/XP clients that use mixed case passwords need to use NetServer passwords.
2* **[CERTIFIED]**	User profile passwords with a length of 1 – 128 characters are supported.
3	User profile passwords with a length of 1 – 128 characters are supported. i5/OS NetServer passwords for Windows 95/98/ME clients will be removed from the system.

*Password level 2 or higher uses SHA1 (the strongest algorithm available in the OS) which renders the passwords unreadable. This SHA1 algorithm meets the PCI consideration for strong encryption.

2. System i passwords must be at least 4 characters long.

System Value	Description
QPWMINLEN	You can use this system value to specify the minimum length of the password.

3. System i passwords to be changed at least every **90** days.

System Value	Description
QPWDEXPITV	You can use this system value to specify when a password expires.

4. System i passwords to include both numeric and alphabetic characters.

System Value	Description
QPWDRQDDGT	You can use this system value to require that passwords use at least one numeric character.

5. New System i password is different than any of the last **4** passwords used.

System Value	Description
QPWDRQDDIF	You can use this system value to specify when a password can be used again.

6. System i limits repeated access attempts by locking out the user account after not more than **6** logon attempts.

System Value	Description
QMAXSIGN	You can use this system value to specify how many incorrect sign-on attempts a user is allowed.

7. System i should disable the user profile when the maximum number of sign-on attempts is reached.

System Value	Description
QMAXSGNACN	You can use this system value to specify the action to take when the maximum number of sign-on attempts is reached.

8. System i should require the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes.

System Value	Description
QINACTITV	You can use this system value to specify in minutes how long the system allows a job to be inactive before taking action.
QINACTMSGQ	You can use this system value to specify what action the system takes when the inactive job time-out interval for a job has been reached.

We recommend that as part of the logon process to the System i, the merchant (distributor) should configure the user profile to immediately display the Distribution iBusiness (A+) default menu to the user. Within the user profile, this is accomplished by completing the "*Initial Program to Call"* field with the *APLUS6P* command. Additionally, the Register A+ User ID's (MENU XACFIG) option is used in order to allow the merchant (distributor) to assign the "*Default Environment"* and "*Default Menu"* to that user. Setting the "*Point of Sale User"* flag to "Y" will bring a POS user directly into POS entry.

The System i user profile may also be restricted to not allow users to key commands on the command line and only allow the selection of provided menu options, by using the "*Limit"* capabilities field.

Additional System i Password Security System Values (Optional)

- QPWDLMTAJC: Limit Adjacent Digits in Password
- QPWDLMTCHR: Limit Characters in Password
- QPWDLMTREP: Limit Repeating Characters in Password
- QPWDMAXLEN: Maximum Password Length
- QPWDMINLEN: Minimum Password Length

Distribution iBusiness (A+) Security Options

Within Distribution iBusiness (A+), there are a few levels to secure users once logged on to the application. The first option grants access to the application through Register iBusiness (A+) User IDs (MENU XACFIG).

The second level is through Application Authority (MENU XASCTY) which allows or denies menu/option access to a specific user or user group, all users, or no users. The third level is Application Action Authority (MENU XASCTY) which further defines access to specific functionality within menu/options.

Specifically for Electronic Payments related to credit card processing, there are 4 additional levels of security to a specific user or user group, all users, or no users:

- Allow Access to Credit Card Inquiry
- Allow Access to Credit Card Numbers in EP Inquiry
- Allow Access to Maintain EP Status
- Allow Access to Credit Card Numbers in Maintenance

Properly Train and Monitor Admin Personnel

It is the merchant (distributor) responsibility to institute proper personnel management techniques for allowing specific user access to cardholder data, site data, etc. You can control whether each individual user can see the credit card primary account number (PAN) or only the last 4 digits via the Application Action Authority options mentioned in the previous section.

In most systems, a security breach is the result of unethical personnel. So pay special attention to whom you trust in Distribution iBusiness (A+) and who you allow to view full decrypted and unmasked payment information.

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

4.1.b: Distribution iBusiness (A+) has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of Distribution iBusiness (A+) in any way will result in non-compliance with PCI DSS.

The PA-DSS logging functionality of this payment application is a combined effort between application logging within Distribution iBusiness (A+), as well as using IBM-specific QHST history logging and file journaling functionality.

The following assessment trails will be logged within Distribution iBusiness (A+)

10.2.1 All individual user accesses to cardholder data:

- Allow access to credit card number in EP inquiry.
- Allow access to credit card numbers in maintenance.
- Allow access to maintain EP status.

10.2.2 All actions taken by any individual with root or administrative privileges:

- Actions recorded within company/system credit card options including:
  - Changing days of credit card transaction history to keep.
  - Changing timeout value.
  - Changing settlement wait time.
  - Changing days until re-encrypt account numbers notification.
  - Changing email distribution group.
  - Adding a new company credit card option record.
  - Adding a new system credit card option record.
- Actions recorded in customer credit card maintenance including:
  - Changing any value within the existing customer credit card record.
  - Adding a new customer credit card record.
  - Deleting an existing customer credit card record.
- Actions recorded in merchant ID maintenance for Interface ‘3’ (Payflow Pro by PayPal) and Interface ‘4’ (PAYware Transact by VeriFone Systems) ***only***, including:
  - Changing the description.
  - Changing the interface setting.
  - Changing the type setting.
  - Changing the credit card customer number.
  - Changing manually close batch during settlement flag.
  - Changing any setting related to either interface 3 or 4.
  - Adding a new merchant ID record.

- Actions recorded in a payment type flagged as a credit card including:
    - Changing the expiration days.
    - Changing the merchant ID.
    - Changing the AVS or CVV flags.
    - Changing the credit card type.
    - Adding a new credit card payment type record.
- Running the re-encrypt account numbers option.
- Running the purge/export security log option.

10.2.3 Access to application audit trails managed by or within the application

- The application audit trail created by Distribution iBusiness (A+) only writes new records to the log, or deletes old records that are purged via Purge/Export EP Security Log (Menu EPFILE) – option 30. At no time within the application would a user be able to update a record within this log. The following steps provided will outline how to journal the EP security logging file in order to determine if a user attempted to update this log (with more than read-only access):
    - To create a journal receiver, the following commands should be typed. Only a qualified, experienced IBM System i user should perform these steps:
        - **CRTJRNRCV JRNRCV(QGPL/EPSLOGJR) THRESHOLD(*NONE)**
    - To create a journal for this journal receiver:
        - **CRTJRN JRN(QGPL/EPSLOGJ) JRNRCV(QGPL/EPSLOGJR) MNGRCV(*USER)**
    - To start journaling the file (omitting open and closing of it), type the following command:
        - **STRJRNPF FILE(EPSLOG) JRN(QGPL/EPSLOGJ) OMTJRNE(*OPNCLO)**
    - If you need to end the journaling at a later time, you can do so by:
        - **ENDJRN OBJ((EPSLOGJ *INCLUDE))**

The following assessment trails will be logged via IBM System i built-in logging functionalities:

10.2.4 Invalid logical access attempts:

- Any failed login attempt is recorded in the QHST history log (IBM).

10.2 5 Use of the application's identification and authentication mechanisms

- Any successful login is recorded in the QHST history log (IBM).

10.2.6 Initialization of the application audit logs

- Both the application specific logging and the QHST history log (IBM) will contain an initialization record for the audit logs.

10.2.7 Creation and deletion of system-level objects within or by the application

- IBM's primary source for auditing information on the system is by way of the security audit journal it provides. A security auditor inside or outside your organization can use the auditing function provided by the system to gather information about security-related events that occur on the system.

Whether viewing the Distribution iBusiness (A+) log, or the IBM system QHST log or file journaling, the above assessment trails will track each event using the following record fields (when applicable):

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

4.4.b: Distribution iBusiness (A+) facilitates centralized logging.

The following option should be run in order to both purge and export the Distribution iBusiness (A+) EP security log into a CSV (comma separated values) format:

- Purge/Export EP Security Log (Menu EPFILE) – option 30.
- The CSV file, in the format ***<current date>.csv***, should reside on the IFS (Integrated File System) in the directory '/EPSecurityLog' on the System i after running option 30.

The following System i commands need to be manually entered in order to export the QHST history log into a CSV format. Only a qualified, experienced IBM System i user should perform this process.

- To send the QHST log to a spool file, type the following command:
  - **DSPLOG LOG(QHST) OUTPUT(*PRINT)**
- To retrieve the attributes of this spool file, type:
  - **WRKSPLF SELECT(*CURRENT *ALL *ALL *ALL *ALL QPDSPLOG)**
    - Enter option 8=Attributes next to the most recently generated QHST spool file and mark down the <*job*>, <*user*>, and <*number*>, as you will need this for a later command.
- Create a physical file in QTEMP to temporarily store the log from the spool file:
  - **CRTPF FILE(HSTLG/QTEMP) RCDLEN(133) MAXMBRS(*NOMAX) SIZE(*NOMAX) LVLCHK(*NO)**

- Copy the log from the spool file into this physical file. You can replace the *LAST with the actual job number if it isn't the last spool file generated:
    - **CPYSPLF FILE(QPDSPLOG) TOFILE(HSTLG/QTEMP) JOB*(<number>/ <user>/ <job>*) SPLNBR(*LAST)**
- From a command line, type:
    - **STRSQL**
- When the 'Enter SQL Statements' display shows, type:
    - **CREATE TABLE QTEMP/HSTLG2 (F1 CHAR (133) CCSID 37 NOT NULL)**
- Copy the records into HSTLG2 table:
    - **CPYTOIMPF FROMFILE(HSTLG/QTEMP) TOFILE(HSTLG2/QTEMP) FROMCCSID(37) DTAFMT(*FIXED)**
- Export the history log onto the IFS on the System i:
    - **CPYTOIMPF FROMFILE(HSTLG2/QTEMP) TOSTMF('/EPSecurityLog/hstlog.csv') MBROPT(*REPLACE) STMFCODPAG(*PCASCII) RCDDLM(*CRLF) STRDLM(*NONE)**
- The ***hstlog.csv*** file should reside on the IFS in directory '/EPSecurityLog'.

The following System i commands need to be manually entered in order to export the journal for the EP security log file into a CSV format. Only a qualified, experienced IBM System i user should perform this process.

- To send the EP security log file journal to a spool file, type the following command:
    - **DSPJRN JRN(QGPL/ESPLOGJ) FILE((EPSLOG *FIRST)) OUTPUT(*PRINT)**
- To retrieve the attributes of this spool file, type:
    - **WRKSPLF SELECT(*CURRENT *ALL *ALL *ALL *ALL QPDSPJRN)**
        - Enter option 8=Attributes next to the most recently generated EPSLOG file journal spool file and mark down the <*job*>, <*user*>, and <*number*>, as you will need this for a later command.
- Create a physical file in QGPL to temporarily store the log from the spool file:
    - **CRTPF FILE(JRNEPSLOG/QGPL) RCDLEN(133) MAXMBRS(*NOMAX) SIZE(*NOMAX) LVLCHK(*NO)**
- Copy the log from the spool file into this physical file. You can replace the *LAST with the actual job number if it isn't the last spool file generated:
    - **CPYSPLF FILE(QPDSPJRN) TOFILE(JRNEPSLOG/QGPL) JOB*(<number>/ <user>/ <job>*) SPLNBR(*LAST)**
- From a command line, type:
    - **STRSQL**
- When the 'Enter SQL Statements' display shows, type:
    - **CREATE TABLE QGPL/JRNEPSLG2 (F1 CHAR (133) CCSID 37 NOT NULL)**

- Copy the records into JRNEPSLG2 table:
  - **CPYTOIMPF FROMFILE(JRNEPSLOG/QGPL) TOFILE(JRNEPSLG2/QGPL) FROMCCSID(37) DTAFMT(*FIXED)**
- Export the history log onto the IFS on the System i:
  - **CPYTOIMPF FROMFILE(JRNEPSLG2/QGPL) TOSTMF('/EPSecurityLog/jrnepslog.csv') MBROPT(*REPLACE) STMFCODPAG(*PCASCII) RCDDLM(*CRLF) STRDLM(*NONE)**
- The ***jrnepslog.csv*** file should reside on the IFS in directory '/EPSecurityLog'.

The following System i commands need to be manually entered in order to export the security audit journal into a CSV format. Only a qualified, experienced IBM System i user should perform this process.

- The security audit journal can be very large so it is recommended to first display the journal prior to setting output to *print. That way, you can view the log section you want to export and indicate a starting/ending date and time. This will make the export more manageable. For this example, to send the security audit journal to a spool file, type the following command:
  - **DSPJRN JRN(QSYS/QAUDJRN) OUTPUT(*PRINT)**
    - Additional note – the QAUDJRN contains many journal codes for many different journal entry types, such as 'D' for database file operations. You can specify the specific job code entry to limit the log. View the following link for more information concerning the security audit journal:

  http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzamv%2Frzamvusesecauditjournal.htm
- To retrieve the attributes of this spool file, type:
  - **WRKSPLF SELECT(*CURRENT *ALL *ALL *ALL *ALL QPDSPJRN)**
    - Enter option 8=Attributes next to the most recently generated security audit journal spool file and mark down the <*job*>, <*user*>, and <*number*>, as you will need this for a later command.
- Create a physical file in QGPL to temporarily store the log from the spool file:
  - **CRTPF FILE(SYSAUDIT/QGPL) RCDLEN(133) MAXMBRS(*NOMAX) SIZE(*NOMAX) LVLCHK(*NO)**
- Copy the log from the spool file into this physical file. You can replace the *LAST with the actual job number if it isn't the last spool file generated:
  - **CPYSPLF FILE(QPDSPJRN) TOFILE(SYSAUDIT/QGPL) JOB*(<number>/ <user>/ <job>*) SPLNBR(*LAST)**
- From a command line, type:
  - **STRSQL**
- When the 'Enter SQL Statements' display shows, type:
  - **CREATE TABLE QGPL/SYSAUDIT2 (F1 CHAR (133) CCSID 37 NOT NULL)**

- Copy the records into JRNEPSLG2 table:
  - **CPYTOIMPF FROMFILE(SYSAUDIT/QGPL) TOFILE(SYSAUDIT2/QGPL) FROMCCSID(37) DTAFMT(*FIXED)**
- Export the history log onto the IFS on the System i:
  - **CPYTOIMPF FROMFILE(SYSAUDIT2/QGPL) TOSTMF('/EPSecurityLog/sysaudit.csv') MBROPT(*REPLACE) STMFCODPAG(*PCASCII) RCDDLM(*CRLF) STRDLM(*NONE)**
- The ***sysaudit.csv*** file should reside on the IFS in directory '/EPSecurityLog'.

Whether from Distribution iBusiness (A+), or using System i commands on the System i for QHST logging, journaling the EP security log file, or for the security audit journal, the CSV files that are exported will reside in the IFS directory '/EPSecurityLog'. The Distribution iBusiness (A+) CSV file can then be imported as text into Excel as comma separated. Meanwhile, the output files from IBM logs can be imported as text into Excel, and adjusted for fixed width using the Excel's import wizard.

Services and Protocols (PA-DSS 5.4.c)

Distribution iBusiness (A+) does not require the use of any insecure services or protocols. Here are the services and protocols that Distribution iBusiness (A+) does require:

- SSL
- HTTPS

Security configuration is embedded within Distribution iBusiness (A+). For example, PayPal provides a certificate for SSL connectivity to their gateway. Also VeriFone Systems provides security connections to payment networks.

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

Distribution iBusiness (A+) does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed per PCI Data Security Standard 2.1.1, 1.2.3, and 4.1.1. In addition, any Distribution iBusiness (A+) merchant using wireless technologies must implement the SSL connection when using Client Access, and/or via A+ GUI (JWalk).

The installing customer needs to consider these 5 points as they consider their wireless environment.

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

1. Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions
2. Default SNMP community strings on wireless devices must be changed
3. Default passwords/passphrases on access points must be changed
4. Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks

5. Other security-related wireless vendor defaults, if applicable, must be changed

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

Standard 4.1.1: Industry best practices (for example, IEEE 802.11.i) must be used to implement strong encryption for authentication and transmission of cardholder data.

Note: The use of WEP as a security control was prohibited as of June 30, 2010.

Never store Cardholder Data on internet-accessible systems (PA-DSS 9.1.b)

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

PCI-Compliant Remote Access (10.2)

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

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

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

Distribution iBusiness (A+) delivers patches and updates in a secure manner with regard to the following points:

- Service Packs are delivered approximately every 120 days. The Service Packs contain fixes and enhancements that have gone through Quality Assurance process and code review based on SDLC process.
- ISO images are created and submitted to Infor Order Fulfillment process and are loaded on Infor Download Center portal.
- The Infor Download Center is accessible by HTTPS and based on Customer authority on access. This encrypted HTTP transfer allows direct download from a web browser, and HTTPS is the only option when a company firewall blocks the FTP protocol. The MD5 signature verifies that the download has been un-tampered.
- Each Service Pack goes through CORE (Critical Operation Review & Evaluation) and Regression testing and as part of the submission of ISO images to the Infor Download Center.

Once we identify a relevant vulnerability for the Distribution iBusiness (A+) application, we work to develop and test a fix/patch that helps protect against the new, specific vulnerability. We attempt to publish a fix/patch based on the issue priority.

Priority descriptions:

- 1-Critical: System is down and business cannot function in any way. This should only be used in extreme circumstances where a turn-around needs to happen within 1-2 days.
- 2-High: Lost functionality that is critical to the customer's business or Data Integrity problem that causes a customer to not be able to run their business with no reasonable work around. Fix should be available within 10 business days.
- 3-Medium: Lost functionality with a reasonable work around. Fix should be available within 20 business days.
- 4-Low: Cosmetic, help text changes, or minor problems. Not a threat to the normal running of the business. Fix should be available within 30 business days.

Once the fix is completed, a "fix" text file is attached to the customer support issue and notification is sent to the customer that the issue is resolved.

We do not deliver software and/or updates via remote access to customer networks. Instead, software and updates are available by logging onto the Infor Download Center, accessible by HTTPS and based on customer authority on access.

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

Infor does this by:

- Subscribing to the IBM partner program whereby we will receive alerts for any IBM vulnerabilities. IBM provides PTFs to address any vulnerability with IBM operating system (OS) problems.

PCI-Compliant Remote Access (10.3.2.b)

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment need to use third-party remote access software such as IBM i Access for Windows, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment).

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

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

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

IBM made security updates in the IBM i7.1 operating system to provide for 128-bit SSL connections with Client Access. The System i must be using the IBM i7.1 operating system and you also must have System i Navigator v7r1m0. Follow IBM's instructions for accessing the Digital Certificate Manager (DCM), creating the SSL certificate, downloading the SSL certificate, and creating SSL secured Client Access sessions.

Data Transport Encryption (PA-DSS 11.1.b)

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

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

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

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

Refer to the Dataflow diagrams for an understanding of the flow of encrypted data associated with Distribution iBusiness (A+). Distribution iBusiness (A+) transactions are not sent across open, public networks. Both Payflow Pro by PayPal and PAYware Transact by VeriFone Systems provide the secure transport of cardholder data across open and private networks to the processors. VeriFone, for instance, will use SSL3, VPN, or a frame-relay/lease line connection.

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

Distribution iBusiness (A+) does not allow or facilitate the sending of primary account numbers (PAN) via any end user messaging technology (for example, e-mail, instant messaging, or chat).

Non-console Administration (PA-DSS 12.1)

Distribution iBusiness (A+) allows non-console administration, so you must use VPN for encryption of this non-console administrative access.

Network Segmentation

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

- Refer to the standardized Network diagram for an understanding of the flow of encrypted data associated with Distribution iBusiness (A+).

Maintain an Information Security Program

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

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

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

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

Distribution iBusiness (A+) started implemented changes for PCI compliance with version 08.01. Customers should plan on updating to the current release of Distribution iBusiness (A+) if they are at a version lower than version 08.03.01. The Electronic

Payments module installs as part of the Order Entry module so there is no additional installation step required.

The Electronic Payments module is licensed separately so after the installation/update of Distribution iBusiness (A+), the security code will be entered. The sheet with the license key provides the instructions to load the key by entering a command to launch a prompt menu where the license key will be entered.

Payment Application Initial Setup & Configuration

For customers installing or activating Electronic Payments the first time, the following steps will need to be completed. Refer to the Distribution iBusiness (A+) Electronic Payments User Guide for more detailed information.

Electronic Payments Setup Checklist

What To Do	Menu and Option
□ Set the *Use Credit Cards* field to Y in Order Entry Options Maintenance.	MENU XAFILE - Order Entry Options Maintenance
□ Define the company options for each company that will use Electronic Payments. ○ Define hold codes pending authorization, expired authorization, processing error, and declined credit card ○ Authorization buffer ○ Days of credit card transaction history to keep ○ Timeout value ○ Settlement report output queues and wait time ○ Default commodity code	MENU EPFILE - Credit Card Options Maintenance
□ Define the application action authority for the quick payment feature and application authority for the EP Transaction Inquiry.	MENU XASCTY – Application Action Authority Maintenance and Application Authority Maintenance
□ Define a “phantom” customer for each credit card/ACH merchant that you want to update to accounts receivable.	MENU ARFILE - Customer/Ship-to Master Maintenance
□ Define merchant IDs for the credit card processing entities.	MENU EPFILE - Merchant ID Maintenance
□ Define a payment type for each type of credit card that you will accept and for ACH/check payments.	MENU ARFILE – Payment Types Maintenance
□ Define credit cards for your customers.	MENU EPFILE - Customer/Ship To Credit Card Maintenance
□ Define bank accounts for your customers.	MENU EPFILE – Customer Bank Account Maintenance
□ Activate Electronic Payments for each company that will use Electronic Payments.	MENU EPFILE – Activate Credit Card Company Options

We recommend that the implementation testing guidelines of the authorization networks be followed.

Payment Application Software Update Setup & Configuration

For customers with Electronic Payments installed and updating to the version recommended (08.03.01) for PCI Compliancy, the following steps will need to be completed.

Credit Card Encryption PCI Compliance

Run the Re-Encrypt Account Numbers (MENU EPFILE) option to allow you to activate Advanced Encryption and perform regular updates to encryption keys. Advanced Encryption will encrypt the credit card account number, expiration date, and cardholder name/address using 256-bit AES encryption. All keys will be generated randomly for each transaction and encrypted data and keys will be stored securely under Key Encryption and Master Data Keys. Keys can be properly managed by system administrators by periodically running this option to re-encrypt cardholder data under new keys account data.

Additionally, outdated cardholder data can be purged from Distribution iBusiness (A+) by entering the appropriate value in the *Purge Data Greater than ____ days old* field on the Re-Encrypt Credit Card Numbers Screen.