



**Payment Application Best Practices (PABP)
Secure Implementation Guide
For
Credit Card Direct™ by Multi-Systems, Inc. (MSI)**

**Implementation Guide
Document Version 1.4
July 24, 2008**

Overview

The Credit Card Direct™ (“CC Direct”) application is developed for use as a processing application for the Lodging industry. Multi-Systems, Inc. has created the CC Direct application to offer a solution that operates in accordance with Visa’s Payment Application Best Practices (PABP), and is subject to an independent third-party audit of the actual CC Direct software application.

Visa U.S.A. Inc. has deployed “Payment Application Best Practices,” referred to in this document as “PABP,” to address security and the risks associated when full magnetic stripe data or CVV2 values are stored during or after the authorization process by payment software applications. This set of practices is designed to assist software developers and application providers in deploying secure software programs that also help merchants to fully comply with Visa’s Cardholder Information Security Program (“CISP”).

Product Design

Credit Card Direct has three main jobs.

- 1) Securely store credit card information entered from an **outside application*. Encryption and other methods secure the data.
- 2) Act as a secure interface between the stored data and the outside application. To do so, Credit Card Direct sends tokens across a secure socket. Thus, the outside application uses a token instead of storing actual credit card data.
- 3) Act as a secure interface between Credit Card Direct and an outside credit card processor or middleware application. This includes obtaining authorizations and submitting payment records.

**Credit Card Direct is interfaced to Multi-Systems, Inc. (“MSI”) hotel property management systems (“PMS”). A PMS is required to process payments with Credit Card Direct 1.0 and is outside of PABP scope. Compatible PMS applications store no sensitive cardholder data that would qualify the PMS as a payment application.*

Property Management System Compatibility

Property Management Systems compatible with Credit Card Direct 1.0:

***Multi-Systems, Inc. WinPM™ version 2.0 & higher
Multi-Systems, Inc. Nova Plus™ version 3.02 & higher***

Product Certification Status

“PABP” Validation: The MSI CC Direct product was designed to meet the requirements of PABP. This product has been evaluated by TrustWave Corporation, an independent auditing corporation. CC Direct is listed on Visa’s list of validated (PABP) payment applications, available at Visa.com, effective March 15, 2008.

“PCI” Compliant: Standalone software products are not evaluated as “PCI” compliant. PCI-DSS standards were developed to assist merchants in developing an overall program to aggressively protect cardholder data from breach of data security. The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Document Purpose

This PABP Implementation Guide contains recommendations made by Multi-Systems, Inc. for proper use of the CC Direct payment application. Multi-Systems, Inc. does **not** possess the authority to state that a merchant may be deemed “PCI-DSS Compliant” if specific directives are followed. Each merchant is uniquely responsible for creating a PCI-compliant environment for which to operate within. The purpose of this Guide is to provide sufficient information regarding the installation and operation of the MSI CC Direct application in a manner that will support a merchant’s PCI-DSS compliance efforts.

Implementation

I. Do not retain Full Magnetic Stripe or CVV2 Data

PABP 1.1.4.A

Data will not need to be purged from any previous version of Credit Card Direct as this application is a new software offering. Credit Card Direct 1.0 replaces legacy payment applications; Credit Card Direct 1.0 does NOT replace a previous version of the same software application.

Notes:

- ❖ The MSI Credit Card Direct product accepts transactions containing magnetic stripe data. This information is transmitted directly to credit card processors and is never stored.
- ❖ Credit Card Direct 1.0 intercepts all incoming magnetic stripe data, acting as a secure interface between the stored data and the outside application. To do so, Credit Card Direct distributes data “tokens” across a secure socket. Thus, the outside application uses a “token” instead of storing any actual credit card data.
- ❖ Merchants should avoid recording credit card numbers in any software application that has not been subject to PABP.
- ❖ Credit Card Direct performs all processing, authorization, and batch settlement functions. Credit Card Direct acts as a secure interface to an outside credit card processor.

II. Protect Stored Account Data: Key Management and Data Cleansing

PABP 1.1.5.A

Data Encryption Key Management:

Secure removal of any cryptograms, encryption keys, or any cryptographic material stored previously by the Credit Card Direct software is an absolute requirement for an MSI customer to operate in a PCI-DSS compliant manner.

The management of encryption keys will be provided by MSI and require no user action by MSI Customers (merchants). Annual key updates will be prompted by the Central Security and Configuration Server (CSCS) located at the MSI facility.

All cryptographic material from previous versions will be completely over-written during the key update process initiated by the CSCS. Software updates will additionally replace any modified cryptographic material. Neither process requires action on the part of the merchant.

Should a compromise be suspected, the merchant or card company can request that MSI invalidate and replace the encryption key at any time. A merchant may contact the MSI Customer Assistance Center at (800) 246-9674 to request an encryption key change if the merchant is led to believe that such a change is necessary.

The key changeover process will at no time leave the data in an unencrypted state.
Notes:

- ❖ The application utilizes TLS (SSL) encryption for all API communications between WinPM and CC Direct and between CC Protect and CC Direct.
- ❖ The CC Direct database utilizes proprietary three-level encryption hierarchy, illustrated by Appendix B; p.15 (Figure 2) of this Implementation Guide.
- ❖ Cryptographic material from previous software versions will be removed in their entirety by the MSI installation process with no additional action required by the merchant.

One component of the Credit Card Direct 1.0 Software Installation Program (CCDirectCustomUninstall.exe) includes deletion of any cryptographic elements from previous versions that may have been installed. MSI customers do not need to undertake any manual operation to ensure the removal of this data in relation to MSI software.

MSI strongly recommends that merchants refrain from manually entering any cardholder data into any text files or free-form fields in any application.

Merchants are responsible for the removal or “sanitation” of any documents or text files that have been manually created which may contain cardholder data.

Protect Stored Account Data: Key Management and Data Cleansing (Continued)

PABP 1.1.6.C

Application Troubleshooting Recommendations:

Software support agents should only be provided with access and to sensitive authentication data to resolve issues that specifically require access to the data to resolve a specific problem.

If any sensitive authentication data is required to be stored by a vendor or support agent, sensitive data should be limited, and stored in a specific and known location with limited access. If sensitive authentication data is stored, data must be encrypted and securely deleted immediately after use.

III. Use of Secure Passwords

PABP 3.1.C

Administrative system accounts:

Merchants are advised not to install software that requires administrative system accounts that do not utilize “strong” passwords. A strong password should appear to be a random string of characters to an attacker. Such a password should be a minimum of eight characters, and include a combination of uppercase and lowercase letters, numbers, and symbols.

Credit Card Direct utilizes the following password guidelines:

- ❖ Password must be at least 8 characters long.
- ❖ Password must contain both numeric and alphanumeric characters.
- ❖ Password can not be re-used within last four (4) password changes.
- ❖ Password expires in 90 days.
- ❖ Users are locked out of the Credit Card Direct Settlement application after three (3) failed attempts. The user is locked out from access for a period of thirty (30) minutes.
- ❖ If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

MSI also suggests that merchants not utilize administrative or other system accounts. Administrative system accounts should not be used for application logins. If possible, any accounts not used should be deleted or disabled. Merchants may utilize an online tool provided by Microsoft to test password strength:

<http://www.microsoft.com/protect/yourself/password/checker.aspx>

IV. Facilitate Secure Network Implementation

PABP 3.2

MSI recommends that our customers follow these guidelines as a minimum standard:

- A. Do not use group, shared, or generic accounts and passwords.
- B. Change your passwords at least every 90 days.
- C. Passwords must be at least 7 characters long.
- D. Passwords must contain both numeric and alphanumeric characters.
- E. Passwords can not be re-used within the last 4 changes.
- F. Repeated attempts at access result in the account being locked.
- G. Account lockdown will be for at least 30 minutes.
- H. Idle sessions will be automatically logged out after 15 minutes.

All computer access accounts should be created and managed following these guidelines.

V. Application User: Log Application Activity

PABP 4.2.B

MSI Credit Card Direct CISP compliant logging is not customer configurable, there is no action required by the customer for this functionality.

VI. Protection of Wireless Transmissions

PABP 6.1.C



The utilization of wireless networks is outside the scope of MSI implementation thus is not recommended, approved or supported by MSI.

If Credit Card Direct is integrated into a merchant system using any wireless application, the merchant must address the PCI-DSS requirements, such as:

- A. Use of approved encryption technologies such as Wi-Fi Protected Access (WPA).
- B. Change wireless vendor defaults, including but not limited to: a) Wired equivalent privacy (WEP) keys, b) Default service set identifier (SSID), c) Disable SSID broadcasts, d) Default passwords, e) SNMP community strings and f) Verify Logging/Auditing is enabled Refer to PCI-DSS for more information on protecting wireless transmissions.
- C. Installing personal firewall software (such as ZoneAlarm) on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
- D. Removal of any default keys from affected wireless equipment
- E. Transmission of cardholder data over a wireless network is not approved by MSI. Wireless networks transmitting cardholder data, per PCI DSS, require encryption of transmissions by using WiFi protected access technology. Merchants should never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, PCI DSS dictates the use of the following:
 - ❖ Use with a minimum 104-bit encryption key and 24 bit-initialization value
 - ❖ Ensure one of the following encryption methodologies is in place for any wireless transmissions: Virtual Private Network (VPN), Secure Sockets Layer (SSL) at 128 bit, or WEP (Wired Equivalency Protocol) at 128 bits.
 - ❖ Rotate shared WEP keys quarterly (or automatically if the technology permits)
 - ❖ Rotate shared WEP keys whenever there are changes in personnel with access to keys
 - ❖ Restrict access based on media access code (MAC) address.
- F: Update virus protection programs to include wireless virus signatures.

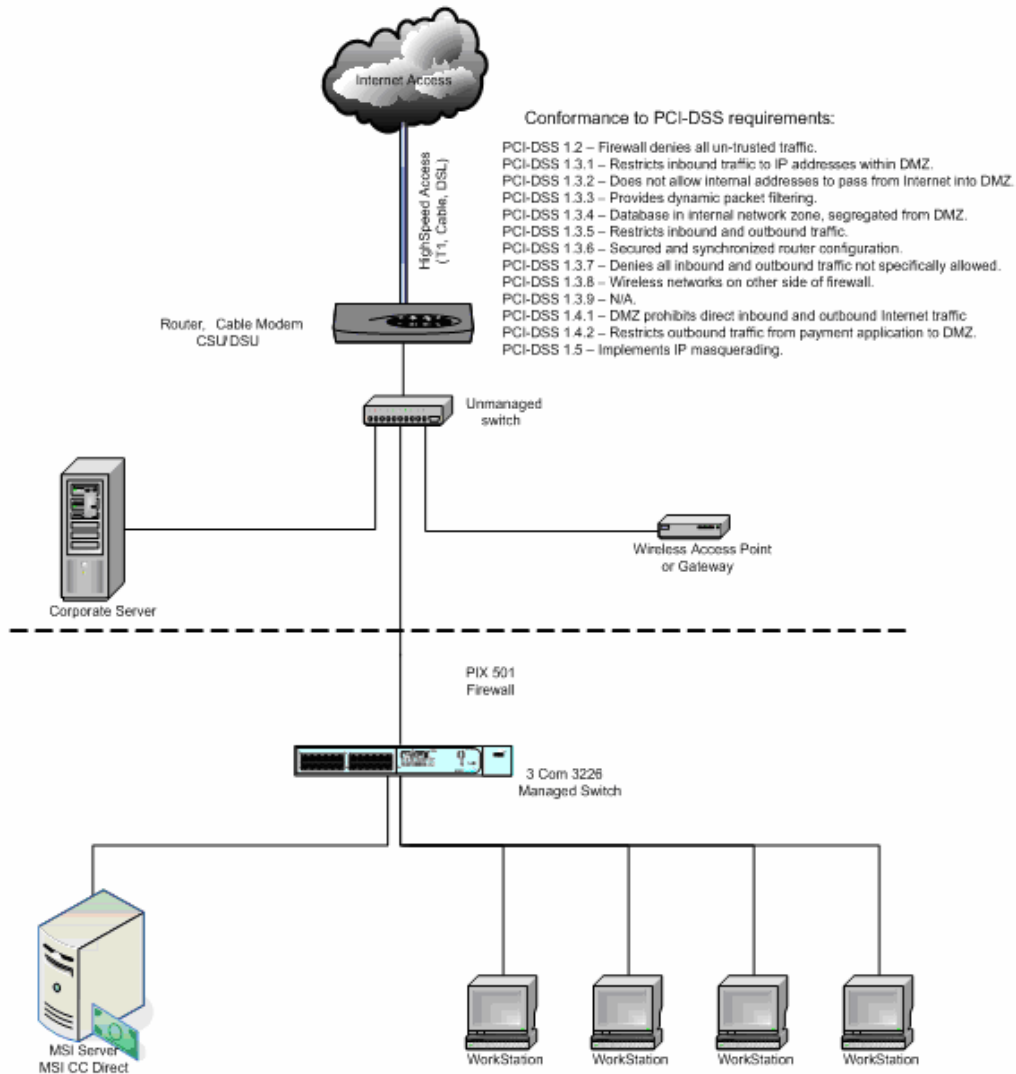
VII. Storage of Cardholder Data - Do Not Store on Server with Web Access

PABP 9.1.B

MSI recommends that Credit Card Direct not be installed on an Internet accessible system. In cases where customer requires presence of a “web server” they should be installed on separate physical computers.

Figure 1

MSI Recommended
 Network Configuration



VIII. Facilitate Secure Remote Software Updates

PABP 10.1

MSI recommends that all MSI software delivery and updating be provided via VPN utilizing the MSI recommended network configuration specified in Figure 1 which conforms to PCI-DSS standards. (cf. Figure 1 p. 9)

MSI recommends that merchants establish an internal policy and / or standard operating procedure with employees pertaining to allowing remote access for software updates or upgrades. Such a usage policy should include consideration of the following PCI security standards (cf. PCI DSS v1.1 section 12.3) for user technologies:

- ❖ Explicit management approval for software upgrades
- ❖ Authentication for use of the technology
- ❖ List of all such devices and personnel with access
- ❖ Labeling of devices with owner, contact information, and purpose
- ❖ Acceptable uses of the technologies
- ❖ Acceptable network locations for the technologies
- ❖ List of company-approved products
- ❖ Automatic disconnect of modem sessions after a specific period of inactivity
- ❖ Activation of modems for vendors only when needed by vendors, with immediate deactivation after use
- ❖ When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.

Multi-Systems, Inc. will assist merchants in maintaining these standards through customer support practices implemented in direct response to PABP section 10.1.

IX. Remote Access to Credit Card Direct Software

PABP 11.2

Credit Card Direct applications are designed to be accessed by a user on a single, local server. If remote access is given to a server or local machine running the Credit Card Direct product, merchants are recommended to regulate access to Credit Card Direct with a secure "challenge/response" mechanism that must be utilized, or no access is granted.

The challenge/response mechanism should be a two-factor authentication that prompts a user for a user and complex password, plus an additional authentication item prior to accessing the Credit Card Direct product.

X. MSI access to Customer servers via Remote Access Software

PABP 11.3.B

MSI recommends that customer work with MSI to perform an audit of existing support software configurations to insure conformance to the new PCI-DSS based guidelines.

MSI recommends that all MSI software support be provided via VPN utilizing the MSI recommended network configuration specified in Figure 1, which conforms to PCI-DSS standards.

Support access to CC Direct is implemented with a secure "challenge/response" mechanism that must be utilized or no access is granted. Each CC Direct instance generates a unique one time only access request challenge which is entered into the central secure support system located at MSI. A validated MSI employee enters the challenge in the system and receives a one time only response that is entered in the CC Direct system at the merchant location. This response contains unique and encrypted information that fully authenticates the MSI support person, and provides authorization for support access for a duration not exceeding an hour.

Please refer to Appendix A - MSI Customer Support Practices

This section will address PABP initiatives related to remote system support and PCI DSS password requirements.

XI. Secure Data Transmission over Public Networks

PABP 12.1

Credit Card Direct 1.0 is intended and designed for deployment on a local merchant's private network. Exposure to a public network is not in the scope of product design; as such, sensitive cardholder data is not transmitted over a public network.

XII. Sending Credit Card Account Numbers via Email

PABP 12.2.B

Credit Card Direct has no capacity to email card holder data, credit card numbers, or sensitive information. Applications that that may be interfaced to Credit Card Direct that may have email capabilities have absolutely no access to credit card numbers or sensitive data.

It must still be recommended to MSI customers (merchants) and strongly stated that credit card numbers or sensitive data should never be transmitted via email in any unencrypted form.

XIII. Non-Console Administration of Credit Card Direct

PABP 13.x

MSI recommends that all MSI software support be provided via VPN utilizing the MSI recommended network configuration specified in Figure 1, which conforms to PCI-DSS standards.

Support access to CC Direct is implemented with a secure "challenge/response" mechanism that must be utilized or no access is granted. Each CC Direct instance generates a unique one time only access request challenge which is entered into the central secure support system located at MSI. A validated MSI employee enters the challenge in the system and receives a one time only response that is entered in the CC Direct system at the merchant location. This response contains unique and encrypted information that fully authenticates the MSI support person, and provides authorization for support access for a duration not exceeding an hour.

XIV. PABP Implementation Guide - Distribution & Corporate Contact Information

Multi-Systems, Inc. will distribute this PABP implementation guide to customers directly through Multi-Systems' customer website:

www.msolutions.com/knowledgecenter.htm

The PABP Implementation guide will be utilized in the training of MSI customers regarding the use of the Credit Card Direct product, which is used for processing credit card payments. MSI's Training and Implementation teams will use the guide to construct training plans consistent with the recommendations contained with the PABP Implementation Guide.

Contact Information

**Customer Assistance Center
Multi-Systems, Inc.**

7600 North 15th Street
Phoenix, Arizona 85020
Toll-Free Customer Support: (800) 246-9674
help@msolutions.com

Corporate Office: (602) 870-4200
info@msolutions.com

www.MsiSolutions.com

APPENDIX A - MSI Customer Support Practices

- (1) Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer)

MSI's Customer Assistance Center create unique passwords for each customer, and advise the customer that in order to use MSI's software and products in a PCI compliant manner, MSI customers will need to duplicate the setup with a unique password for each workstation they wish to grant access to MSI software. Passwords will be stored in MSI's SupportLogix application, accessible only to MSI associates signed in to a specific support ticket for a specific problem.

- (2) Allow connections only from specific (known) IP/MAC addresses

MSI recommends that all MSI software support be provided via VPN utilizing the MSI recommended network configuration shown in Figure 1 on Page 9 of this Guide.

- (3) Use strong authentication or complex Passwords for logins

Support access to CC Direct is implemented with a secure "challenge/response" mechanism that must be utilized or no access is granted. Each CC Direct instance generates a unique one time only access request challenge which is entered into the central secure support system located at MSI. A validated MSI employee enters the challenge in the system and receives a one time only response that is entered in the CC Direct system at the merchant location. This response contains unique and encrypted information that fully authenticates the MSI support person, and provides authorization for support access for a duration not exceeding an hour.

If an MSI customer requires assistance in creating "strong" passwords, one example of an online password generator may be found at:

<http://onlinepasswordgenerator.com/password.cgi>

- (4) Enable encrypted data transmission

MSI will activate data encryption in PCAnywhere (Symantec) when the MSI Team dials in to set up unique passwords. MSI customers may contact MSI Support at (800) 246-9674 to inquire regarding whether data encryption has been activated for MSI support sessions using the Symantec PCAnywhere software product.

- (5) Enable account lockout after a three (3) failed login attempts

Lockout is activated in Symantec PCAnywhere. MSI customers may contact MSI Support at (800) 246-9674 to inquire regarding whether account lockout has been activated for MSI support sessions using the Symantec PCAnywhere software product.

- (6) Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed

MSI recommends that all MSI software support be provided via VPN utilizing the MSI recommended network configuration specified in Figure 1, which conforms to PCI-DSS standards.

(7) Enable the logging function

MSI customers may contact MSI Support (Customer Assistance Center) to ensure that logging is activated for PCAnywhere software support sessions required to address a specific problem.

(8) Restrict access to customer Passwords to authorized reseller/integrator personnel

Support access to CC Direct is implemented with a secure "challenge/response" mechanism that must be utilized or no access is granted. Each CC Direct instance generates a unique one time only access request challenge which is entered into the central secure support system located at MSI. A validated MSI employee enters the challenge in the system and receives a one time only response that is entered in the CC Direct system at the merchant location. This response contains unique and encrypted information that fully authenticates the MSI support person, and provides authorization for support access for a duration not exceeding an hour.

(9) Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5.

If an MSI customer requires assistance in creating "strong" passwords, one example of an online password generator may be found at:

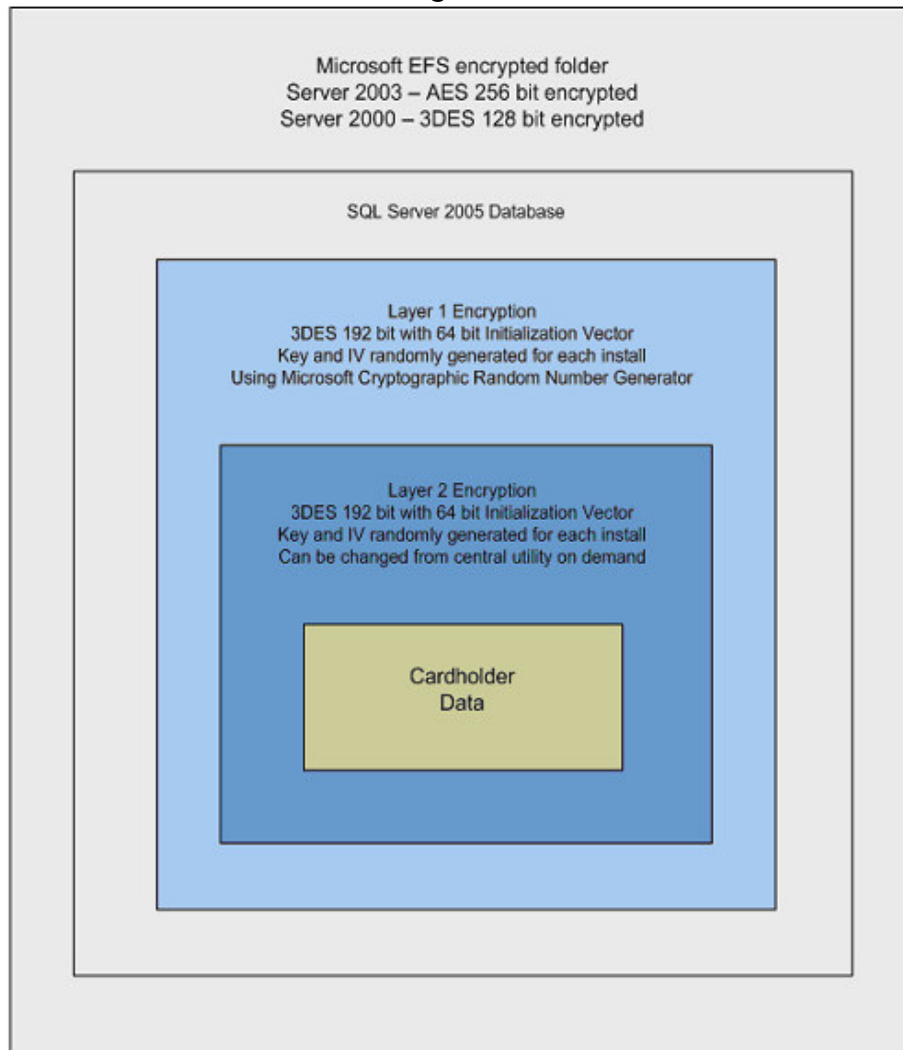
<http://onlinepasswordgenerator.com/password.cgi>

APPENDIX B - Diagram of MSI Credit Card Direct 1.0 Encryption Scheme

The MSI Credit Card Direct database is encrypted at three levels to offer maximum protection in a secure environment (Figure 2).

- ❖ Entire database is level 1 encrypted via AES 256 bit encrypted folder.
- ❖ Cardholder data is level 2 encrypted by Triple-DES 192 bit key and 64 bit Initialization Vector that is randomly generated and unique for each install.
- ❖ Cardholder data is level 3 encrypted by Triple-DES 192 bit key and 64 bit Initialization Vector that is randomly generated and unique for each install, and can be updated on demand by central management utility.

Figure 2



APPENDIX C - Removal of Legacy Backups and Training Materials

Multi-Systems, Inc. has created the CC Direct application to offer a solution that operates in accordance with Visa's Payment Application Best Practices (PABP).

If upgrading from previous Property Management Systems (PMS) or payment application software that may store either "prohibited" data (or permitted sensitive data in unencrypted form), it is strongly recommended that any databases from previous versions of these products be removed.

If assistance is needed in determining whether sensitive information remains on a system from a previous or legacy software system, please contact MSI Support at (800) 246-9674 to assist you in this process.

APPENDIX D - Transaction Diagram: Credit Card Direct 1.0 with Hotel PMS

Figure 3 displays a diagram of the secure interface between Credit Card Direct and a credit card processor or middleware application, in tandem with a hotel property management system.

Credit Card Direct sends “tokens” across a secure socket. A token is a data string that serves as unique representation of a credit card number in a secure database; a token contains no sensitive cardholder information.

The PMS application uses a token, instead of storing actual credit card data.

