

Visual Ticket 10.1

PA-DSS Implementation Guide

Version 0.1

Approval Date: [01/21/2010]

Document Owners

Cyrus Nima

President/Developer

Microcode Corp.



Confidential Information

The information contained in this document is Microcode Corp. confidential and has been prepared to establish internal policies and procedures. Distribution of this document outside of Microcode Corp. is strictly prohibited. Do not copy or distribute without the permission of the Chief Technoloav

Table of Contents

Notice.....	3
About this Document.....	4
Revision Information.....	5
Executive Summary.....	6
Application Summary.....	6
Typical Network Implementation.....	8
Dataflow Diagram.....	8
Difference between PCI Compliance and PA-DSS Validation.....	9
Considerations for the Implementation of Payment Application in a PCI-Compliant Environment.....	10
Remove Historical Credit Card Data (PA-DSS 1.1.4.a).....	10
Sensitive Authentication Data requires special handling (PA-DSS 1.1.5.c).....	10
Purging of Cardholder Data (PA-DSS 2.1.a).....	11
Removal of Cryptographic material (PA-DSS 2.7.a).....	11
Set up Good Access Controls (3.1.c and 3.2).....	11
Properly Train and Monitor Admin Personnel.....	12
Key Management Roles & Responsibilities (PA-DSS 2.5).....	12
Log settings must be compliant (PA-DSS 4.2.b).....	12
PCI-Compliant Wireless settings (PA-DSS 6.1.b and 6.2.b).....	13
Never store cardholder data on internet-accessible systems (PA-DSS 9.1.b).....	14
PCI-Compliant Delivery of Updates (PA-DSS 10.1).....	14
PCI-Compliant Remote Access (11.2 and 11.3.b).....	15
Data Transport Encryption (PA-DSS 12.1.b).....	16
PCI-Compliant Use of End User Messaging Technologies (PA-DSS 12.2.b).....	16
Network Segmentation.....	16
Maintain an Information Security Program.....	17
Application System Configuration.....	17
Payment Application Initial Setup & Configuration.....	Error! Bookmark not defined.

Notice

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. MicroCode Corp. 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 MicroCode Corp. 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, MicroCode Corp. 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 Visual Ticket 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 1.2 dated October, 2008).

MicroCode Corp. instructs and advises its customers to deploy MicroCode Corp. applications in a manner that adheres to the PCI Data Security Standard (v1.2). 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.

If you do not follow the steps outlined here, your Visual Ticket installations will not be PA-DSS compliant.

Revision Information

Name	Title	Date of Update	Summary of Changes
Cyrus Nima	President/Developer	01/15/2009	Initial 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. MicroCode Corp. will distribute the IG to customers via both as a condition of the download of the PA-DSS condition version and it will also be available on the vendor website.

Executive Summary

Payment Application version 10.1 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 1.2. 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 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>

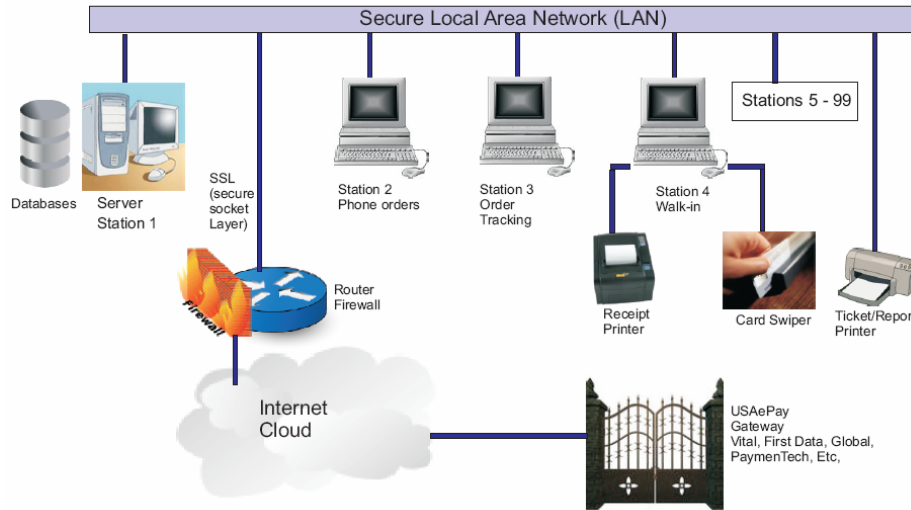
Application Summary

Name:	Visual Ticket
Application Version Number(s):	10.A1
Components of Application (ie. POS, Back Office, etc):	Vft.exe Main program that includes the credit card functionality, but is primarily for managing flower shop orders and other store functionality including billing, delivery, production tracking, etc. Agent.exe Runs various routines that are not credit card related (such as item management, file maintenance, backups, email reminders, etc.)
Credit Card Server(s):	Xauthorize.dll A secure channel to send Credit Card information to a

	gateway. Vendor only sends to the USA ePay gatgeway.
Other Required Third Party Software:	None
Setup:	Setup_NT.EXE
Operating Systems:	Windows XP Pro SP3, Vista and 7
Code base, DB engine:	Visual Fox Pro 8.0 – Service Pack 2
Application Description:	Visual Ticket is designed to support a merchant in floral and gift basket companies, and for the customers that need credit card processing it will also support credit card processing through USA ePay. It runs in a server only or client server environment depending on the customer's needs.
Application Environment	Server or client server
Application Target Clientele:	Retail floral shops and gift basket companies.
Description of Versioning Methodology:	Visual Ticket versioning has three levels, Major, Minor, and Release: X.X.X. Major changes include significant changes to the application and would have an effect on PA-DSS requirements. Minor changes include small changes such as minor enhancements and may or may not have an effect on PA-DSS requirements. Release date changes include bug fixes, cosmetic and user Interface changes that would have no affect on PA-DSS requirements.

Typical Network Implementation

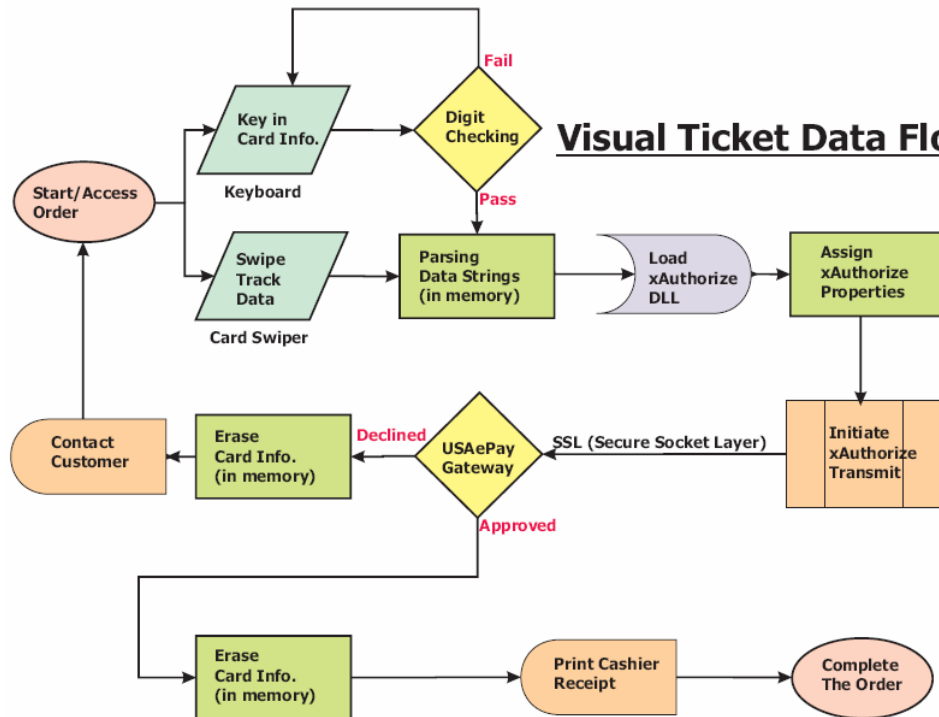
Visual Ticket Secure LAN Diagram



- Visual Ticket stations run their Executables from the local Drive, while accessing the Server for Data only.
- Card Info is never saved on Disk.
- Track Data is never saved on disk.

Dataflow Diagram

Visual Ticket Data Flow Diagram



Difference between PCI Compliance and PA-DSS Validation

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

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

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

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

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

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

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

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

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

- 7. Restrict access to data by business need-to-know*
- 8. Assign a unique ID to each person with computer access*
- 9. Restrict physical access to cardholder data*

Regularly Monitor and Test Networks

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

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

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

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






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

Remove Historical Credit Card Data (PA-DSS 1.1.4.a)

Previous versions of Visual Ticket did not store sensitive authentication data. Therefore, there is no need for secure removal of this historical data by the application as required by PA-DSS v1.2.

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

The following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

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

Note: Visual ticket does have memo fields and other generic fields that you could input this type of data into and in order to stay PCI compliant you should NEVER input any credit card data into these fields. If you have any concerns that you may have done this or are not sure which fields this might include please contact us immediately.

Purging of Cardholder Data (PA-DSS 2.1.a)

Visual Ticket (version 10.A) does not store cardholder data and therefore there is no data to be purged as required by PA-DSS v1.2.

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

Visual Ticket has the following versions that previously encrypted cardholder data: Version 9 or earlier and the following must be done:

- ✘ All cryptographic material (encryption keys and encrypted cardholder data) must be securely removed.
- ✘ To securely remove this material you must upgrade to 10.1A or higher and the upgrade process will automatically remove all cryptographic material.
- ✘ This removal is absolutely necessary for PCI DSS Compliance
- ✘ Visual Ticket no longer stores cardholder data.

Setup Good Access Controls (3.1.c and 3.2)

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. The following should be followed:

- ✘ Do not use administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).
- ✘ Assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts.
- ✘ Assign strong application and system passwords whenever possible.
- ✘ Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standard 8.5.8 through 8.5.15
- ✘ Changing the "out of the box" settings for unique user IDs and secure authentication will result in non-compliance with the PCI DSS

The PCI standard requires the following password complexity for compliance (often referred to as using "strong passwords"):

- ✘ Do not use group, shared, or generic user accounts (8.5.8)
- ✘ Passwords must be changed at least every 90 days (8.5.9)
- ✘ Passwords must be at least 7 characters (8.5.10)
- ✘ Passwords must include both numeric and alphabetic characters (8.5.11)
- ✘ New passwords cannot be the same as the last 4 passwords (8.5.12)

PCI user account requirements beyond uniqueness and password complexity are listed below:

- ✘ If an incorrect password is provided 6 times the account should be locked out (8.5.13)
- ✘ Account lock out duration should be at least 30 min. (or until an administrator resets it) (8.5.14)
- ✘ Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session (8.5.15)

These same account and password criteria must also be applied to any applications or databases included in payment processing to be PCI compliant. Visual Ticket, as tested to in our PA-DSS audit, meets, or exceeds these requirements.

Visual Ticket must require unique usernames and complex passwords for all administrative access and for all access to cardholder data.

[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.]

- ✘ Control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Properly Train and Monitor Admin Personnel

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

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

Key Management Roles & Responsibilities (PA-DSS 2.5)

Visual Ticket does not store cardholder data in any way nor does it provide any configurability that would allow a merchant to store cardholder data.

Log settings must be compliant (PA-DSS 4.2.b)

Visual Ticket has PA-DSS compliant logging enabled by default by providing relevant data to USAePay. This logging is not configurable and may not be disabled. Disabling or subverting the logging function of Visual Ticket in any way will result in non-compliance with PCI DSS.

Visual Ticket provides any possible logs to USAePay to help support the following per PCI DSS 10.2 and 10.3 as follows:

Implement automated assessment trails for all system components to reconstruct the following events:

- 10.2.1 All individual user accesses to cardholder data*
- 10.2.2 All actions taken by any individual with root or administrative privileges*
- 10.2.3 Access to all assessment trails*
- 10.2.4 Invalid logical access attempts*
- 10.2.5 Use of identification and authentication mechanisms*
- 10.2.6 Initialization of the assessment logs*
- 10.2.7 Creation and deletion of system-level objects.*

Record at least the following assessment trail entries for all system components for each event from 10.2.x:

- 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.*

Disabling or subverting the logging function of Visual Ticket in any way will result in non-compliance with PCI DSS.

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

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

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.

2.1.1:

- ☒ All wireless networks implement strong encryption (e.g. AES)*
- ☒ Encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes positions*
- ☒ Default SNMP community strings on wireless devices were changed*
- ☒ Default passwords/passphrases on access points were changed*
- ☒ Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2)*
- ☒ Other security-related wireless vendor defaults, if applicable*

4.1.1:

- ☒ Industry best practices are used to implement strong encryption for the following over the wireless network in the cardholder data environment (4.1.1):*

- Transmission of cardholder data
- Transmission of authentication data
- ✍ Payment applications using wireless technology must facilitate the following regarding use of WEP:
- ✍ For new wireless implementations, it is prohibited to implement WEP as of March 31, 2009.
- ✍ For current wireless implementations, it is prohibited to use WEP after 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 Delivery of Updates (PA-DSS 10.1)

Visual Ticket delivers updates via a secure process as follows:

- Timely development and deployment of patches and updates. Visual Ticket deploys patches and updates within 3 days.
- Delivery in a secure manner with a known chain-of-trust and that maintains the integrity of the deliverable. Visual Ticket delivers updates via SFTP and the update.exe delivered is created by Xitech Konxise to encrypt the update.
- Integrity testing of patches or updates prior to installation.

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

We do this by:

Regularly monitoring both Fox Pro Development Forums and Visual Studio Development forums.

Once we identify a relevant vulnerability, we work to develop & test a patch that helps protect Visual Ticket against the specific, new vulnerability. We attempt to publish a patch within 3 of the identification of the vulnerability. We will then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install available patches within 30 days.

Most updates are done by a Visual Ticket employee on site with a USB device or CD. However, in some cases we deliver software and/or updates via remote access to customer networks.

This is only done through the secure methods provided through “Goto Assist Express” (For Visual Ticket Users who call the Visual Ticket Support line). This method requires a customer personnel to be onsite and grant access to a Visual Ticket employee by entering a one-time use 9 digit code provided over the phone.

For Visual Ticket Users who call the Floral Systems (the Only Reseller) Support line, the Remote Connection is done through the similar secure methods provided by “Secure Webx” which also requires that a customer personnel to be onsite to grant access to a Floral Systems employee by entering a one-time 9 digit code “Meeting Number” which is provided over the phone.”

For receiving updates via remote access, merchants must adhere to the following guidelines:

- ✘ Secure remote access technology use, per PCI Data Security Standard 12.3.9:
12.3.9 Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use

Customers must properly configure a firewall or personal firewall product.

PCI-Compliant Remote Access (11.2 and 11.3.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 may need to use third-party remote access software such as “Goto Assist” 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). Additionally, the PCI user account and password requirements will apply to these access methods as well.

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

- ✘ Change default settings (such as usernames and passwords) on remote access software (e.g. VNC)
- ✘ Allow connections only from specific IP and/or MAC addresses
- ✘ Use strong authentication and complex passwords for logins according to PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- ✘ Enable encrypted data transmission according to PCI DSS 4.1
- ✘ sdaEnable account lockouts after a certain number of failed login attempts according to 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 PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

Data Transport Encryption (PA-DSS 12.1.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.

- ✘ Refer to the Dataflow diagram for an understanding of the flow of encrypted data associated with Visual Ticket.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 12.2.b)

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

Non-console administration (PA-DSS 13.1)

Visual Ticket does not allow or support non-console administration.

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 Visual Ticket.

Maintain an Information Security Program

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

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

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

Application System Configuration

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

- ▣ Microsoft, Windows XP Professional with Service Pack 3. All latest updates and hot-fixes should be tested and applied.
- ▣ 512 MB of RAM minimum, 2GB or higher recommended for Payment Application
- ▣ 400 MB of available hard-disk space
- ▣ TCP/IP network connectivity

3rd Party Shopping Cart support

Visual ticket has a component called the VOX Agent which downloads completed web orders via SFTP from 3rd Party Shopping Carts. This only occurs after the payment on such orders is already processed in real time prior to import. No Card Holder data is imported / transferred via the VOX Agent.

It is the responsibility of the customer to insure that the Shopping Cart deployed is PA_DSS Certified.

USAePay Gateway Configuration

In order to maximize Batch Control and prevent any unauthorized / inaccurate Card transactions, the "Settlement Control" (Auto Close Batches) on USAePay's "Settings" menu, should be set to "Never".

This setting would then require that the System Manager / Owner to always review the "Current Batch" before it is Settled (Closed). See screenshot below.

The screenshot shows the USAePay Console Settings interface. At the top, it displays the date and time: "Tue January 19, 2010 13:58:22 PST" and navigation links: "Support | Visual Ticket | LogOut". The USAePay logo is on the left, and "Console Settings Member Control Panel" is on the right. Below the header, it shows "MicroCode Corp. - DEMO" and "User: visualticket". A navigation menu includes "Home", "vTerminal", "Sale Form", "Customers & Billing", "Batches", "Reports", "Search", "Settings", and "Fraud Center". A secondary menu includes "General", "Users", "Source Keys", "Receipts", "Custom Fields", and "Change Password". The "Settings" section is active, showing "MicroCode Corp. - DEMO".

System Settings

Merchant Email	<input type="text"/>
Report Rows/Page	<input type="text" value="20"/>
Use Compact Mode	<input type="checkbox"/>

Batch Settings

Auto Close Batches Every:	<input type="text" value="Never"/>
Send Batch Reports To:	<input type="text"/>
Send Batch Errors To:	<input type="text"/>
Expire Auths After:	<input type="text" value="10 Days"/>