C680

PCI PTS POI Security Policy

Revision A.2

C680 PCI PTS POI SECURITY POLICY

Contents

PREFACE

This guide is the primary source of information for technicians, administrators and site managers who will deploy and manage the C680 series terminals.

AUDIENCE

This guide is useful for the following users:

- **Entities deploying C680 terminals to end user sites**

  Performs specific tasks required to deploy new C680 terminals into the field, such as:

  - Terminal configuration
  - Application software download
  - Testing of the terminal prior to deployment

- **Administrators or Site Managers**

  Performs administrative and on-site duties, such as:

  - Change passwords
  - Perform routine tests and terminal maintenance
  - Configure terminals for remote diagnostics and downloads

ORGANIZATION

This guide is organized as follows:

Chapter 1, Introduction. Provides an overview of this Security Policy.

Chapter 2, Firmware and Application Maintenance. Provides information on System Mode and Application Download procedures.

Chapter 3, Security Policy. Provides information on how to securely deploy C680 terminals.

C680 PCI PTS POI SECURITY POLICY

CHAPTER 1

INTRODUCTION

This Security Policy provides guidance for the proper and secure usage of Payment Card Industry (PCI) Payment Terminal Security (PTS) Approved Point of Interaction version 4.0 devices, such as the C680 terminal series.

SCOPE

The security policy applies to the C680 terminals, which is PCI PTS version 4.x POI approved. Failure to use the terminal in accordance with this security policy will cause the terminal to not be in compliance to the PCI PTS POI Modular Security Requirements version 4.0 approval of the device.

PRODUCT IDENTIFICATION AND INSPECTION

Carefully inspect the shipping carton and its contents for possible tampering or damage.

1. Validate the authenticity of the sender by verifying the shipping tracking number and other information located on the product order paperwork.
2. Remove the C680 unit from the shipping carton.
3. Remove all plastic wrapping from the unit and other components.
4. Remove the clear protective film from the display.
5. Save the shipping carton and packing material for future repacking or moving the device.

To verify if your C680 product is PCI approved as a PED (PIN Entry Device), locate the PCI Identification number at the bottom of the device. Go to the PCI Security Standards Council web site (www.pcisecuritystandards.org) and verify that the PCI Hardware Version matches the **Hardware #** on the list of Approved PIN Transaction Security (PTS) Devices.

Figure 1, C680 Terminal

The following illustration shows the location of the hardware ID (PCI Hardware Version) on the product label.

Figure 2, Match the PCI Hardware Version listed on the device

You must also verify that your C680 product is running a PCI PED approved Operating System and IP Stack (identified as OP) . Shortly after powering up, a splash screen displays the version number for the Operating System. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices just as was done for the Hardware identifier. If these numbers do not match, notify your service provider immediately. In this example, the Operating System version number is "**QT680450**" that agrees with approved Firmware version number **"QTyy0450"**.

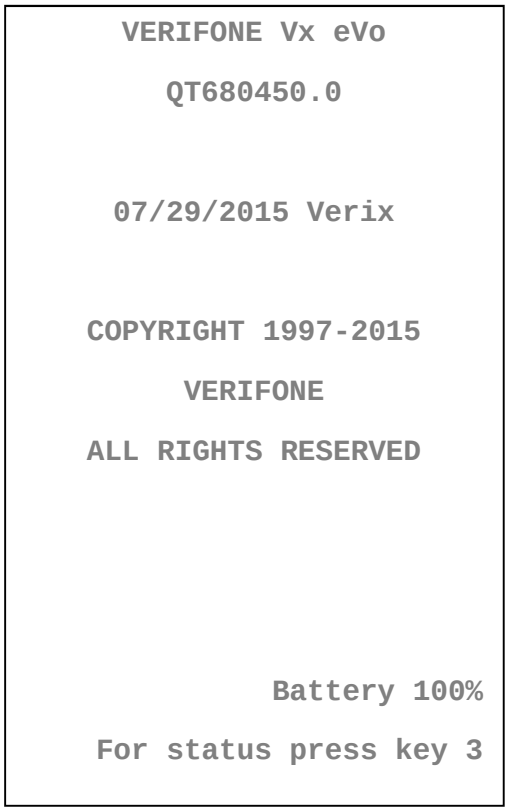

Figure 3, C680 Boot Splash Screen

The IP Stack software version can be obtained by pressing the "5" key during the startup splash screen or from the Verix Terminal Manager "Software Versions menu". The obtained version number must match any of the listed IP stack version numbers for this product. If these numbers do not match, notify your service provider immediately. In this example, the IP Stack software version number is "OP Ver **1.2.0.0**" that agrees with approved Firmware version number "OP: **1.x.x.x**".

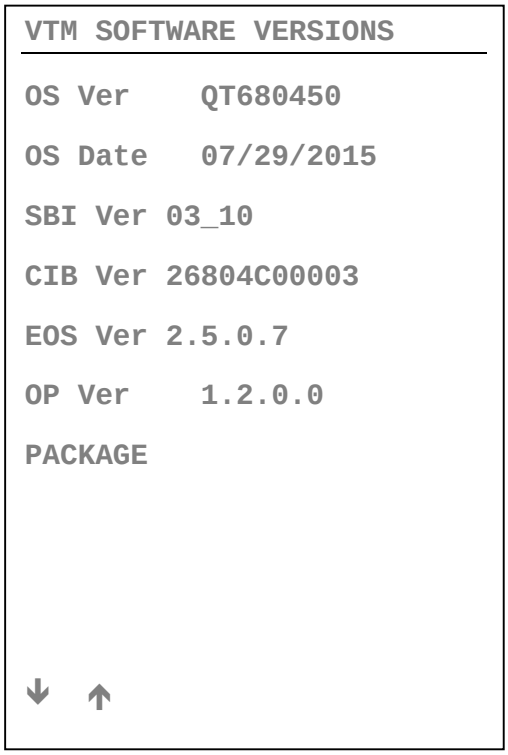

Figure 4, IP Stack Software Version ("OP Ver")

CHAPTER 2

FIRMWARE AND APPLICATION MAINTENANCE

LOCAL OPERATIONS

Local operations within the Verix Terminal Manager (VTM) allows for standalone terminals to perform data transfers between the terminal and another terminal or computer. Perform local VTM operations to configure, test, and display.

For more information about Verix Terminal Manager, refer to Appendix A for the [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).

REMOTE OPERATIONS

Remote operations require communication between the terminal and a host computer over a network connection. Perform remote VTM operations to download application software to the terminal, upload software from one terminal to another, or perform diagnostics over a network.

For more information about Verix Terminal Manager, refer to Appendix A for the [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).

CHAPTER 3

SECURITY POLICY

This policy ensures secure deployment of C680 terminals and complies with the PCI PTS POI standards version 4.x.

ENVIRONMENT

- The C680 has a security architecture called VeriShield Retain, which has both physical and logical components. The logical security component, called File Authentication (FA) is part of the terminal's operating system software.

  File Authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process enables the sponsor of an C680 terminal to logically secure access to the terminal by controlling who is authorized to download applications or firmware updates files to the terminal. It proves and verifies the file's origin, sender's identity and the integrity of the file's information. If any of these three items are not verified, then the download is rejected.

- Prior to usage and deployment, familiarize yourself with the [R7] C680 Installation Guide (DOC269-003-EN-A). This guide provides information on verifying terminal equipment, usage, safety, security, environmental requirements, and troubleshooting steps if needed.

- The C680 must be used in an attended environment.

- The C680 terminals are handover devices. Always exercise extreme caution when conducting transactions especially during PIN entry:

- Hand the C680 directly to the cardholder for PIN entry.

- Encourage the cardholder to hold the C680 close to avoid others to see the information entered.

- Periodically inspect the terminal for possible tampering. Signs of tampering include:
  - Wires protruding out of the device
  - Foreign objects inserted into the smart card slot or mag stripe slot
  - Signs of damage to the tamper evident labels
  - Warning message on the device display; see Figure 5

- If any device is found in tamper state, please remove it from service immediately, keep it available for potential forensics investigation, and notify your company security officer and your local Verifone representative or service provider. For contacting Verifone, please see section "Verifone Service and Support" in [R7] C680 Installation Guide (DOC269-003-EN-A)

- The following are the temperature and humidity specifications of the C680:
  - Operating temperature: -10° to 50° C (14° to 122° F)
  - Storage temperature: -20° to 70° C (-4° to 158° F)
  - Relative humidity: 5% to 95% (RH non-condensing)

- Subjecting the C680 to extreme environmental conditions will result in tamper events. Any temperatures above 100 degrees Celsius (± 5 degrees) or below -40 degrees Celsius (± 5 degrees) will result in a tamper condition. Additionally, should the backup battery voltage drift outside of the range of 2.3 VDC to 3.8 VDC, the unit will tamper as well.

- The terminal contains no user serviceable parts. Do not, under any circumstances, attempt to disassemble the terminal.

KEY MANAGEMENT

- See items [R1] and [R2] in References for key management techniques supported by the terminal.

- The terminal does not support manual cryptographic key entry. Key injection and management equipment must be managed in a secure manner to minimize the opportunity for compromise in accordance with items [R1], [R2], and [R4] in References.

- Physical keys, authorization codes, passwords, and other credentials must be managed under dual control and split knowledge so that no one person can use two credentials simultaneously.

- Key management security objectives must be in compliance with PCI PIN Transaction Security requirements.

- Employing key management schemes that do not comply with PCI PTS with PCI payments will invalidate the PCI PTS approval for this POI.

- Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information.

The following table lists all supported key management schemes. For more information, refer to [R13] 2.0 Encryption Services Organization Key Management Procedures“.

Key Name	Size (bytes)	Algorithm	Purpose
DUKPT (PIN)	16	DUKPT (ANSI X9.24)	PIN encryption
DUKPT (MAC)	16	(ANSI X9.24) MAC (ANSI X9.19)	Message MAC’ing
Master Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	Encrypt/Decrypt Session Keys from host per Master Session Key Management
Session (PIN) Key	16, or 24	DES (FIPS 46-3, ANSI X3.92, X3.106); TDEA ANSI X9.52)	PIN block encryption
Session (MAC) Key	16	MAC (ANSI X9.19)	Message MAC’ing
Application Signer		RSA 2048 SHA-256	Used by customer to sign Applications to install to device.

ADMINISTRATION SECURITY

- Configuration of the terminal must be performed prior to installation and use. For more information, refer to chapter 4 of the [R7] C680 Installation Guide (DOC269-003-EN-A).
- This configuration mode must limited to administrators and maintenance/support personnel. The administrators should setup the maintenance user prior to installation and use.
- Passwords are pre-expired and must be changed upon first use. These passwords must be at least 7 decimal characters (0-9) in length.
- Updates and/or patches to the operating system can be performed by the administrators using the Verix Terminal Manager. Updates/patches are RSA certificate authenticated. If the signature of the updates cannot be authenticated, the update/patch is rejected and not installed.

- Develop a process that monitors consistently problematic devices, such as high read failures or debit card declined transactions. These are indications of a tampered terminal.

- Implement a policy that requires all repair technicians who visit your store to sign in, verify their identity with photo identification, and remain accompanied by store personnel during any work performed on PIN pads and/or terminals.

- Implement a procedure that checks the terminal serial number every time the device is started or powered on to insure the device has not been replaced. If the device has been replaced, cease using the terminal and notify your Verifone customer relations manager.

- Visually inspect the terminal daily to ensure there are no foreign objects present in the smartcard slot; ensure there are no wires emanating from the smartcard slot.

- Develop a breach response plan. This identifies the steps to take if a suspected breach occurs and as well as who will perform each step. The plan needs to include isolation of your payment systems and a list of all personnel who need to be notified. These personnel include your local law enforcement, your acquiring bank, your processor, security assessor, as well as your payment system vendor.

- Track each instance of replaced terminals within the store. Whether from the in store inventory, by a repair technician or with terminals shipped into the store.

- VeriShield FST (File Signing Tool) manages the generation and signing of device certificates. See DevNet and [R12] VeriShield FST Basics for more information on signing tool implementation.

DEVICE DIAGNOSTICS

- C680 terminals implement a self-test to confirm firmware integrity. The self-test is performed:
    - When the unit powers
    - When the unit is rebooted
    - At least once every 24 hours
    - Upon demand

- Authorized maintenance personnel may configure the C680 to perform self-test at a specified time.

- Authorized maintenance personnel may manually invoke the self-test by entering System Mode, (system mode passwords required), and selecting the self-test option.

- The following components are checked during self-test:
    - Integrity of the TMK (Terminal Master Key)
    - Integrity of the other key files
    - Tamper detection system
    - VeriShield certificate tree
    - Firmware

- If a self-test fails, the C680 limits its functionality based on the severity of the issue discovered. Device response ranges from partial disablement of applications to non-functionality.

DEVICE SECURITY

- Security mechanisms employed within the terminal can detect physical tampering and triggers a tamper event. This causes the terminal to cease performing transactions and indicates that it has been tampered on the device display; see Figure 5.

- Terminal security must not be compromised by altering the environmental conditions. The power and temperature operating ranges should be within the specifications specified in [R7] C680 Installation Guide (DOC269-003-EN-A). Operating the terminal outside of these ranges triggers a tamper event and causes the terminal to cease performing transactions and indicates that it has been tampered on the device display; see Figure 5.

- The terminal must perform a self-test upon start up and at least once per 24 hour period. The operating system performs the self-test automatically and does not require intervention from the user or the application.

- If any device is found in tamper state, please remove it from service immediately, keep it available for potential forensics investigation, and notify your company security officer and your local Verifone representative or service provider. For contacting Verifone, please see section “Verifone Service and Support” in [R7] C680 Installation Guide (DOC269-003-EN-A)

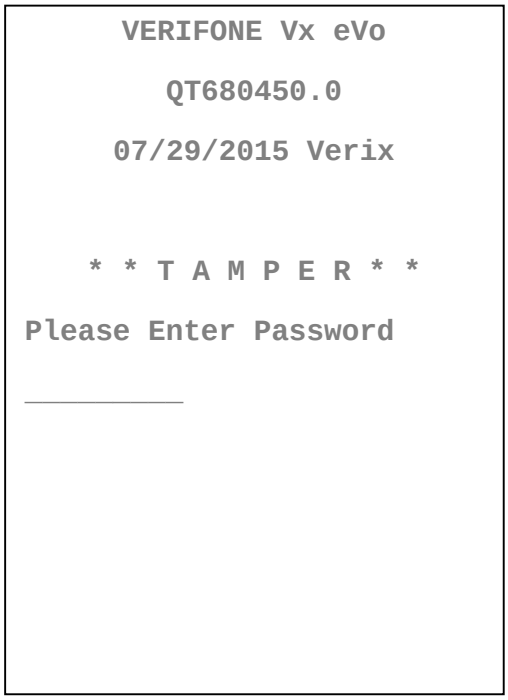

Figure 5, Tampered device message on terminal display

CODERS/DEVELOPERS (Firmware and Application)

- All payment based applications and firmware must undergo a formal review and security audit before they may be signed and used.
    - The reviewer must be a qualified individual who was not involved with the authorship of the POI PED code.
    - Code review must be governed by an auditable process that shows the code review and security testing have been performed, and requires a sign-off by the person(s) performing the code review and security tests.
        - The tester shall confirm that the process will show any problems noted during the code review and security testing
    - Such reviews must happen after each and every code change.
    - The firmware must be reviewed against PCI POI PED requirements, the guidance listed in this document, as well [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301).

- The terminal operating system authenticates the applications prior to execution. The authentication process includes verifying the RSA certificate and signature of the application.

- Applications must be designed and implemented in accordance with the PA-DSS requirements document entitled, [R15] PA-DSS Program Guide v3.0.

- Only application codes that have been authorized for release should be signed and released to the field. The signing must occur under dual control and split knowledge.

- When developing IP capable payment based applications, developers must follow the guidance listed in the following documents:
  - [R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301)
  - [R9] Verix eVo Volume II: Operating System and Communication Programmers Guide (VPN – DOC00302)
  - [R10] Verix eVo IP Stack Security Guidance Users Guide (VPN – DOC00326)
  - This Security Policy
  - [R14] VeriShield File Signing Overview

- All referenced best practices regarding coding practices and device configurations must be followed.

- Transaction data must be cleared as soon as the transaction is completed, including but not limited to working registers and buffers.

- If the product is SRED enabled:
  - The working buffers associated with PAN encryption clears automatically as soon as the transaction completes.
  - The encryption of PAN data is automatic and transparent to your application – there are no added API calls needed.

- Allowable application behavior:
  - Write to the display
  - Fetch keypad entries
  - Request an encrypted PIN block

- Forbidden application behavior:
  - Change PIN entry retry limit
  - Attempt to alter PIN entry time-out.
    - PIN entry time-outs are set and enforced by the OS. The application is not capable of altering these.
    - PIN Entry time-outs are set to: 30 Seconds without key presses, or 300 Seconds with key presses.
  - Modify a key
  - Generate a subordinate certificate
  - Execute another application
  - Encrypt arbitrary data

CRYPTOGRAPHY

- Only use acceptable cryptographic algorithms listed in [R6] SP800-57 Part 1: Recommendation for Key Management.

- The cryptographic strength should be at least 112 bits.

- Cryptographic algorithms used should be at least: SHA-256, 2TDEA, RSA-2048, AES-128.

- Although other cryptographic algorithms may be supported, they may not be used for payment-based applications.

FIRMWARE UPDATES

The C680 supports firmware updates. For more information on performing compliant firmware updates, refer to [R7] C680 Installation Guide (DOC269-003-EN-A).

DECOMMISSIONING/REMOVAL FROM SERVICE

Before removing the device from service permanently or for repairs, all sensitive data must be erased. Sensitive data includes credit card data and all encryption keys inclusive of ALL Private, PIN, Data encryption keys.

If the device is permanently decommissioned from service, it can be done by disassembling the device in order to force a tamper condition, so all sensitive data will be erased automatically. After performing this operation, turn on the terminal and verify that the unit is in tamper state; see the Figure 5.

CHAPTER 4

REFERENCES

[R1] ANS x9.24 Part 1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[R2] ANS x9.24 Part 2:2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[R3] ISO 9564-1, Financial Services Personal Identification Number (PIN) Management and Security Part 1: Basic Principles and Requirements for PIN's in Card-Based Systems
[R4] X9 TR-31:2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[R5] ISO 9564-2, Banking, Personal Identification Number Management and Security Part 2: Approved Algorithms for PIN Encipherment
[R6] SP800-57 Part 1: Recommendation for Key Management
[R7] C680 Installation Guide (DOC269-003-EN-A)
[R8] Verix eVo Volume I: Operating System Programmers Manual (VPN – DOC00301)
[R9] Verix eVo Volume II: Operating System and Communication Programmers Guide (VPN – DOC00302)
[R10] Verix eVo IP Stack Security Guidance Users Guide (VPN – DOC00326)
[R11] Point of Interaction (POI) Modular Security Requirements v4.0
[R12] VeriShield FST Basics
[R13] 2.0 Encryption Services Organization Key Management Procedures
[R14] VeriShield File Signing Overview
[R15] PA-DSS Program Guide v3.0