



delivering comprehensive
payment security experience

Lifecycle of a Secure Payment Device: Post Manufacturing Stage

Revision 3.0

June 6, 2011

Table of Contents

| | | |
|---------|---|----|
| 1 | Overview | 5 |
| 2 | Abbreviations | 6 |
| 3 | Glossary | 7 |
| 4 | Stage Definition | 8 |
| 5 | Stages and Processes | 9 |
| 6 | Assumptions..... | 10 |
| 7 | Stage Security Objectives..... | 11 |
| 8 | Applicable Standards..... | 12 |
| 8.1 | Applicable Standards Security Requirements | 13 |
| 8.1.1 | PIN Transactions Security Version 2.1, January 2009 | 13 |
| 8.1.1.1 | Device Management Requirements | 13 |
| 8.1.2 | ISO 1349 1-1 | 14 |
| 8.1.3 | ISO 13491-2: Annex A. Physical, Logical and Device Management Characteristics Common to All Secure Cryptographic Devices..... | 14 |
| 8.1.3.1 | Device Management..... | 14 |
| 8.1.3.2 | Device Protection between Manufacturer and Pre-use | 14 |
| 8.1.4 | Annex B. Devices with PIN Entry Functionality | 15 |
| 8.1.4.1 | PIN entry Device Protection during Initial Key Loading..... | 15 |
| 8.1.5 | Annex E. Devices with Key Generation Functionality | 15 |
| 8.1.5.1 | Logical Security Characteristics..... | 15 |
| 8.1.6 | Annex F. Devices with Key Transfer and Loading Functionality..... | 16 |
| 8.1.6.1 | Logical Security Characteristics..... | 16 |
| 8.1.6.2 | Device Management..... | 16 |
| 8.1.7 | Annex G Devices with Digital Signature Functionality | 18 |
| 8.1.7.1 | Device Management..... | 18 |

| | | |
|---------|--|----|
| 8.1.8 | Annex H Categorization of Environments | 18 |
| 8.1.8.1 | Minimally Controlled Environments..... | 18 |
| 8.1.8.2 | Controlled Environments..... | 19 |
| 8.1.8.3 | Secure Environments..... | 20 |
| 8.1.9 | PIN Security & TR39 | 21 |
| 8.1.9.1 | PIN Security | 21 |
| 8.2 | Security Requirements Analysis | 22 |
| 8.2.1 | Security Requirements Standards Map | 22 |
| 9 | Lifecycle Protection Methods | 23 |
| 9.1 | ISO 13491-1 Requirements..... | 23 |
| 9.2 | Protection Methods Analysis | 23 |
| 10 | Audit and Control Principles..... | 24 |
| 10.1 | PTS | 24 |
| 10.2 | ISO 13491-1 | 24 |
| 10.3 | ISO 13491-2..... | 25 |
| 11 | Stakeholders | 26 |
| 12 | SPVA Certification Requirements..... | 27 |
| 12.1 | SPVA Security Requirements..... | 27 |
| 12.1.1 | SPVA_Post_Manufacturing_Sec_Req_1 | 27 |
| 12.1.2 | SPVA_Post_Manufacturing_Sec_Req_2..... | 27 |
| 12.1.3 | SPVA_Post_Manufacturing_Sec_Req_3..... | 28 |
| 12.1.4 | SPVA_Post_Manufacturing_Sec_Req_4 | 28 |
| 12.1.5 | SPVA_Post_Manufacturing_Sec_Req_5..... | 28 |
| 12.1.6 | SPVA_General_Req..... | 28 |
| 12.2 | SPVA Audit Control Objectives..... | 29 |
| 12.2.1 | SPVA_Post_Manufacturing_Aud_Req_1 | 29 |
| 13 | Rationale | 30 |

| | | |
|--------|---|----|
| 13.1 | SPVA Security Requirements Map | 30 |
| 13.2 | SPVA Security Requirements Coverage..... | 31 |
| 13.2.1 | Secure Post-Manufacturing Processes | 31 |
| 13.2.2 | Initial Key Loading..... | 31 |
| 13.2.3 | Secure Delivery and Storage | 31 |
| 13.2.4 | Incident Management | 31 |
| 13.2.5 | SPVA AUDIT | 31 |
| 13.3 | SPVA Key loading Scenarios | 32 |
| 14 | References | 34 |
| 15 | Appendix 1 SPVA Requirements Updated After PCI PTS v3. (April 2010) | 35 |
| 15.1 | Introduction | 35 |
| 15.2 | PCI PTS v3 Requirements: Manufacturer and Initial Key Loading..... | 35 |
| 15.3 | SPVA Security Requirements Map | 36 |
| 15.4 | SPVA Certification Requirements..... | 36 |
| 15.4.1 | SPVA_Post_Manufacturing_Sec_Req_2 (Refined)..... | 36 |
| 15.4.2 | SPVA_Post_Manufacturing_Sec_Req_5 (New Requirement) | 37 |

1 Overview

The main purpose of this document is to define the SPVA security requirements applicable for the Post Manufacturing Stage of a payment device.

SPVA has performed a thorough analysis of the current security standards for POS terminals during the Post Manufacturing Stage. The purpose of the analysis was to estimate any potential missing information in security standards in order to achieve full coverage as mandated by the SPVA board. This document represents the conclusions of this effort.

This document only focuses on the Post Manufacturing Stage which covers the moment the terminal has been produced to the moment the terminal is loaded with the customer keys.

The SPVA TWG2 had the following members who worked on this document:

Chairman: Roberto Fañanás, Hypercom. Other members include:

| Organization Represented | Representative | |
|---------------------------------|-----------------------|-----------------|
| Hypercom | Isabel | Bardsley-Garcia |
| Ingenico | Yann | Levenez |
| Mustang MicroSystems, Inc | Tami | Harris |
| Mustang MicroSystems, Inc. | Tom | Galloway |
| PAXSZ | Alex | DongDQ |
| Verifone | Doug | Manchester |
| Verifone | Sadiq | Mohammed |

2 Abbreviations

DES -- A symmetric method known as Data Encryption Standard

ISO -- International Standards Organization

NIST -- National Institute of Standards and Technology

PCI -- Payment Card Industry

PCI SSC-- PCI Security Standards Council

PD -- Payment Device

PED -- POS PIN Entry Device

PTS -- PIN Transaction Security

POS -- Point of Sale

RSA -- An asymmetric method developed by Rivest Shamir and Adelman

SP -- A document from NIST: Special Publication

SPVA -- Secure POS Vendor Alliance

TDEA -- A method using DES three times in sequence (i.e. encrypt-decrypt-encrypt) using two or three keys conforming to the Triple Data Encryption Algorithm.

TWG --Technical Working Group

3 Glossary

Asymmetric Keys -- Comprised of a pair of keys, one Public, the other Private, that are used to accomplish secure communication and authentication. RSA algorithm uses asymmetric keys. More information can be found in X9.24 part 2.

Customer Key -- A key under Customer management responsibility, usually an acquirer.

Initial Key --The key that is used to assure the integrity and authenticity of the PD during the full Lifecycle of a Secure Payment Device.

Initial Key loading -- Process for Customer Key loading.

Payment Device trust establishment -- A process to establish the trust relationship between PD and PD manufacturer.

Symmetric Keys -- Comprised of a single key that is shared between two or more parties and kept secret (i.e. private) used to accomplish secure communications. Symmetric keys can be used for message authentication (i.e. MAC). DES and TDEA are two of several symmetric key methods. More information can be found in X9.24 part 1.

Vendor Keys -- Asymmetric Key pairs under PD manufacturer management responsibility.

4 Stage Definition

The Post Manufacturing Stage consists of the transport and storage of the PD up to and including initial key loading (ISO 13491-1: 2007)

This is the only stage covered in this document. Other stages are defined in the following table with the different transition phases. Some of these other stages will be studied in future SPVA documents for Secure Device Lifecycle Management.

5 Stages and Processes

| Lifecycle Phase | Transition Event | Processes | | | Audit |
|--------------------|---------------------|---|------------------------------|-------------------------------|---------------------------------------|
| Pre-Manufacturing | | | | | |
| Manufacturing | Completion | Secure Manufacturing Processes | | Incident Management Processes | Secure Delivery and Storage Processes |
| Post-Manufacturing | Initial Key Loading | | | | |
| Pre-Use | Installation | Secure Deployment Processes | Secure Development & Updated | | |
| Use | Removal | Secure in-Field Device Management Processes | | | |
| | Re-installation | | | | |
| Post-Use | Repair, upgrade | Device Repair Processes | | | |
| | Destruction | Secure Device Decommissioning Processes | | | |

Main

- Secure Delivery and Storage Processes
- Payment Device Securitization Process (Initial Key Loading)

Related

- Incident Management Process
- Audit Process

6 Assumptions

The moment the Payment Device (PD) reaches the Post Manufacturing Stage, it must be able to perform, at minimum, the following functions:

- Trigger an action as a response to tamper detection
- Load authenticated software

In other words, the PD is a working device with the ability to run authenticated software and the security mechanisms that are required to provide a response to tamper detection.

7 Stage Security Objectives

| | Confidentiality | Integrity | Availability | Accountability | Authenticity | Non-repudiation |
|-------------------------------------|-----------------|-----------|--------------|----------------|--------------|-----------------|
| Secure Post-Manufacturing Processes | | √ | | √ | √ | |
| Initial Key Loading | √ | √ | | √ | √ | √ |
| Secure Delivery and Storage | | | | | √ | √ |
| Incident Management Processes | √ | √ | | √ | √ | |

- **Confidentiality:** Sensitive information is not disclosed to unauthorized individuals, entities, or processes. [ISO-18028-2:2006]
- **Integrity:** Safeguarding the accuracy and completeness of assets. [ISO/IEC ISO-13335-1:2004] [ISO-27001:2005][ISO-13335-1:2004]
- **Accountability:** Actions of an entity may be traced uniquely to the entity. [ISO-7498-2:1989]
- **Authenticity:** Authentic, trustworthy, or genuine.
- **Non-repudiation:** Provides assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party as having originated from a specific entity in possession of the private key of the claimed signatory. [NIST-SP800-57:2007]
- **Availability:** Accessible and useable upon demand by an authorized entity. [ISO/IEC ISO-13335-1:2004] [ISO-18028-2:2006][ISO-27001:2005][ISO-13335-1:2004]

8 Applicable Standards

The main standards that are applied to this stage of the process are defined as follows:

Payment Card Industry (PCI) POS PIN Entry Device Security Requirements (PTS¹) Version 2.1 January 2009:

This document is only concerned with the device management for point-of-sale PEDs up to the point of initial key loading. Subsequent to receipt of the device at the initial key-loading facility, the acquiring financial institution and its agents (e.g., merchants and processors) are responsible for the device and are covered by the operating rules of the *Associations and the PCI PIN Security Requirements*.

ISO 13491-1: 2007 Banking -- Secure cryptographic devices (retail) -- Concepts, requirements and evaluation methods:

ISO 13491 describes both the physical and logical characteristics and the management of the secure cryptographic devices used to protect messages, cryptographic keys and other sensitive information used in a retail financial services environment.

This part of ISO 13491 has two primary purposes:

- To state the requirements concerning both the operational characteristics of SCDs and the management of such devices throughout all stages of their lifecycle, and
- To standardize the methodology for verifying compliance with those requirements.

ISO 13491-2: 2000 Banking -- Security compliance checklists for devices used in magnetic stripe card systems:

This part of ISO 13491 specifies the checklists used to evaluate secure cryptographic devices (SCDs) incorporating cryptographic processes, as specified in ISO 9564, ISO 9807 and ISO 11568, in a magnetic stripe card environment. It does not specify checklists for SCDs used in an integrated circuit card (ICC) environment.

¹ PTS (PIN Transaction Security) former PCI -PED

PCI PIN Security Requirements Version 2.0 January 2008 (Visa):

This document contains a complete set of requirements for the secure management, processing and transmission of Personal Identification Number (PIN) data during online and offline payment card transaction processing at ATMs, and attended and unattended point-of-sale (POS) terminals.

ANSI X9 TR-39-2009. TG-3 Retail Financial Services Compliance Guideline Part 1: PIN Security and Key Management:

The PIN Security Compliance Guideline is intended to be used to implement a uniform security review. This guideline presents mandatory Control Objectives relating to general procedures and controls. The mandatory Control Objectives are based on requirements set forth in the following:

- X9.8-1-2003 Part 1: (Personal Identification Number (PIN) Management and Security)
- X9.24-1-2004 (Retail Financial Services Symmetric Key Management, Part 1: Using Symmetric Techniques)
- X9.24 Part 2: 2006 (Retail Financial Services Symmetric Key Management, Part 2: Using Asymmetric Techniques for Distribution of Symmetric Keys).

8.1 Applicable Standards Security Requirements

8.1.1 PIN Transactions Security Version 2.1, January 2009

8.1.1.1 Device Management Requirements

| | Description of Requirement |
|----|---|
| F1 | The PED is shipped from the manufacturer's facility to the initial-key-loading facility and stored in route under auditable controls that can account for the location of every PED at every point in time. |
| F2 | Procedures are in place to transfer accountability for the device from the manufacturer to the initial-key-loading facility. |
| F3 | While in transit from the manufacturer's facility to the initial-key-loading facility, the device is: <ul style="list-style-type: none">▪ Shipped and stored in tamper-evident packaging; and/or▪ Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial-key-loading facility, but that cannot feasibly be determined by unauthorized personnel. |

8.1.2 ISO 1349 1-1

| No. | Description of Requirement |
|-----|---|
| | <p>Until an initial key has been loaded, it is necessary to detect a compromise but not to prevent it.</p> <p>If a compromise is detected, it is only necessary to ensure that keys are not injected into the device and it is not placed in service until all effects of the compromise have been eliminated from it.</p> |

8.1.3 ISO 13491-2: Annex A. Physical, Logical and Device Management Characteristics Common to All Secure Cryptographic Devices

8.1.3.1 Device Management

| No. | Security compliance statement |
|-----|--|
| A32 | For audit and control purposes, the identity of the device (e.g. its serial number) can be determined, either by external tamper-evident marking or labeling, or by a command that causes the device to return its identity via the interface or via the display. |
| A36 | If a device does not yet contain a secret cryptographic key and there is an attack on a device, or a device is stolen, then procedures are in place to prevent the substitution of the attacked or stolen device for a legitimate device that does not yet contain a secret cryptographic key. |
| A37 | If no sensitive state exists in the device, the loading of plaintext keys will be performed under dual control. |

8.1.3.2 Device Protection between Manufacturer and Pre-use

| No. | Security compliance statement |
|-----|--|
| A40 | The transfer mechanisms by which plaintext keys, key components or passwords are entered into the device are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any component or password. |
| A41 | Subsequent to manufacturing and prior to shipment, the device is stored in a protected area or sealed within tamper-evident packaging to prevent undetected unauthorized access to it. |

| No. | Security compliance statement |
|-----|---|
| A42 | <p>The device is shipped in tamper-evident packaging, and inspected to detect unauthorized access to it; or</p> <ul style="list-style-type: none"> ▪ before a device is loaded with cryptographic keys, it is closely inspected by qualified staff to ensure that it has not been subject to any physical or functional modification; or ▪ the device is delivered with secret information that is erased if tampering is detected to enable the user to ascertain that the device is genuine and not compromised. <p>NOTE: One example of such information is the private key of an asymmetric key pair, with the public key of the device signed by a private key known only to the supplier.</p> |
| A43 | <p>The device is loaded with initial key(s) in a controlled manner only when there is reasonable assurance that the device has not been subject to unauthorized physical or functional modification.</p> |

8.1.4 Annex B. Devices with PIN Entry Functionality

8.1.4.1 PIN entry Device Protection during Initial Key Loading

| No. | Security compliance statement |
|-----|---|
| B20 | <p>A repaired PIN entry device is not reloaded with the original key (except by chance).</p> |
| B21 | <p>Automated techniques are used, or manual procedures are in place and are followed, to ensure each PIN entry device is given at least one statistically unique key unknown to any person and never previously given (except by chance) to any other PIN entry</p> |

8.1.5 Annex E. Devices with Key Generation Functionality

8.1.5.1 Logical Security Characteristics

| No. | Security compliance statement |
|-----|--|
| E2 | <p>The device's key management functions are designed so that no disclosure of any key is possible without collusion between trusted individuals. Specifically:</p> <ul style="list-style-type: none"> ▪ the device's highest-level keys are manually loaded as at least two components under dual control; ▪ any function used to input or output key components does not operate until at least two different passwords have been entered. |

| No. | Security compliance statement |
|-----|---|
| E3 | The device decomposes an actual key into key components in such a way that no “active” bit of the key could be determined without the knowledge of all components. For example, the components are exclusive-or'ed together to form the key. |
| E4 | Key generation methods comply with ISO 11568. |
| E5 | Each call to obtain a generated key yields a different, statistically-unique key (except by chance). |

8.1.6 Annex F. Devices with Key Transfer and Loading Functionality

8.1.6.1 Logical Security Characteristics

| No. | Security compliance statement |
|-----|--|
| F2 | Enciphered private keys are protected against key substitution and modification. |
| F3 | The device's key management functions are designed so that no disclosure of any key is possible without collusion between trusted individuals. Specifically: <ul style="list-style-type: none"> ▪ the device's highest-level keys are manually loaded as at least two components; ▪ any function used to input or output key components, except for the device's components. |

8.1.6.2 Device Management

| No. | Security compliance statement |
|-----|--|
| F9 | The transfer mechanisms by which keys, components or passwords are transferred into or out of the device are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any keys, components or passwords. |
| F14 | Controls are in place to detect the unauthorized removal of the device from, and its unauthorized replacement back into, its authorized location. |
| F15 | The device is loaded with a key component under the direct supervision of a person who is allowed access to this component, and only when there is reasonable assurance that there is no “bug” or other disclosing mechanism on the path that the key component traverses from the key generation device to the transport device itself. |

| No. | Security compliance statement |
|-----|--|
| F16 | If the device contains a plaintext key component, the device is either under the continuous supervision of a person who is allowed access to this component (and who is aware of his/her responsibilities to ensure the secrecy of this component), or else is locked or sealed in a security container that cannot feasibly be opened without detection by anyone other than those who are allowed access to the component. |
| F17 | The device is used to inject a component into a cryptographic device only under the direct supervision of a person who is allowed access to this component, and only when there is reasonable assurance that there is no “bug” or other disclosing mechanism on the path that the key component traverses from the key transport device to the cryptographic device. |
| F18 | <p>The transfer of a key to another secure cryptographic device uses either:</p> <ul style="list-style-type: none"> ▪ a secure communications path, or ▪ a secure key transfer device, or ▪ a secure cryptographic path, or ▪ is carried out in a secure environment. |
| F19 | No person with knowledge of or access to one of the passwords or physical keys required to output a key from the device has knowledge of or access to any other such password or physical key of this device. |
| F20 | The device is loaded with a plaintext key only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism on the path that the key traverses from the key generation device to the key-transport device itself. |
| F21 | The device is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism on the path that the key traverses from the key transport device to the cryptographic device |

| No. | Security compliance statement |
|-----|--|
| F22 | <p>Functionality needed to import, export, or transfer cryptographic keys from external sources ensures that the keys are in one or more of the following forms:</p> <ul style="list-style-type: none"> ▪ enciphered under the proper variant of a symmetric key encipherment key; ▪ enciphered under the asymmetric public key of the recipient; ▪ enciphered with an import key being specifically enabled for a limited time and limited number of function calls; ▪ input under dual or multiple control through the secure operator interface, in components such that full knowledge of all but one component gives no usable information on any bit of the cryptographic key; ▪ public keys are entered under dual control or enciphered under the appropriate key or signed as required to ensure authenticity. |

8.1.7 Annex G Devices with Digital Signature Functionality

8.1.7.1 Device Management

| No. | Security compliance statement |
|-----|--|
| G1 | <p>If non-repudiation is claimed then:</p> <ul style="list-style-type: none"> ▪ the asymmetric private and public key pair is generated within the digital signature device; and ▪ the asymmetric private key is not exported outside the original digital signature device for any reason, including backup and archival purposes. |
| G2 | <p>For audit and control purposes, the binding between the public key and the identity of the owner of the private key is readily determined by use of:</p> <ul style="list-style-type: none"> ▪ public key certificates, where the public key certificate was obtained from an authorized certificate authority, or ▪ public key certificates and appropriate certificate management procedures, or ▪ other equivalent mechanisms to irrefutably determine the identity of the owner of the corresponding private key. |

8.1.8 Annex H Categorization of Environments

8.1.8.1 Minimally Controlled Environments

| No. | Security compliance statement |
|-----|---|
| H1 | <p>Authorized access is restricted by physical locks or supervised access points to authorized staff, and persons accompanied by authorized</p> |

| No. | Security compliance statement |
|-----|--|
| | staff. |
| H2 | The environment provides facilities for secure fastening of devices with lockable fastening mechanisms, if such devices are to be installed. |
| H3 | A minimally controlled environment shall remain intact until all keys and other secret data stored in devices within the environment are destroyed or until all such devices are removed from the environment. |

8.1.8.2 Controlled Environments

| No. | Security compliance statement |
|-----|--|
| H4 | Authorized access is restricted by physical locks and continually supervised access points to authorized staff, and persons accompanied by authorized staff. |
| H5 | Any access by other than authorized staff is logged, and the log securely kept and periodically audited. |
| H6 | <p>The devices are either:</p> <ul style="list-style-type: none"> ▪ in full view at all times of at least two staff members who have been instructed to check the devices for signs of attacks or presence of any other persons at the devices; or ▪ in view of a video camera (through a closed video system) being monitored at least once every X/2 min, or whenever movement close to the devices is automatically detected; by persons who have been specifically tasked with checking the devices for signs of attacks. <p>NOTE: The time “X/2 min” is half the time “X min” which is the time estimated to successfully penetrate the equipment in order to:</p> <ul style="list-style-type: none"> ▪ make any additions, substitutions, or modifications (e.g. the installation of a bug) to the hardware or software of the device; or ▪ determine or modify any sensitive information (e.g. PINs, access codes, and cryptographic keys), and then subsequently reinstall the device, without requiring specialized skills and equipment not generally available, and without damaging the device so severely that the damage would have a high probability of detection. |
| H7 | There are no entry or exit points for people or equipment except for continually supervised access points, e.g. watched by guards who have been instructed not to permit any import or export of equipment without written authorization identifying the equipment, signed by an authorized person other than the person moving the equipment. |
| H8 | It is not feasible to gain unauthorized access to the controlled environment, or import or export equipment, from under the floor or from above the ceiling. |

8.1.8.3 Secure Environments

| No. | Security compliance statement |
|-----|--|
| H9 | Authorized access is restricted by physical locks and continually supervised access points to pairs of authorized staff and persons accompanied by pairs of authorized staff. Access points that are not supervised are locked and alarmed, so that any entry or exit causes intervention by guards. |
| H10 | Any non-authorized person(s) requiring access to the secure environment will be supervised at all times by at least two authorized persons whilst in the secure environment. |
| H11 | All accesses to the secure environment are logged, and the log securely kept and periodically audited. |
| H12 | <p>All possible access points to the secure environment are either:</p> <ul style="list-style-type: none"> ▪ in full view at all times of at least two authorized staff members who have been instructed to check the devices for signs of attacks; or ▪ in view of a video camera (through a closed video system) coupled with circuitry that automatically raises an alarm whenever movement close to the devices is detected or tamper detection circuitry is activated. Even when no alarm is raised, the camera is monitored at least once every 10 min. The images are watched by persons who have been specifically tasked with checking the secure environment for signs of attacks. |
| H13 | There are no entry or exit points for people or equipment except for continually supervised access points, watched by guards who have been instructed not to permit any import or export of equipment without written authorization identifying the equipment, signed by an authorized person other than the person moving the equipment. |
| H14 | If the secure environment is implemented as a secured room, then the device(s) in the secure environment are in view of a video camera (through a closed video system) coupled with circuitry that automatically raises an alarm whenever movement close to the devices is detected or tamper detection circuitry is activated. Even when no alarm is raised, the camera is monitored at least once every 10 min. The images are watched by persons who have been specifically tasked with checking the secure environment for signs of attacks. |
| H15 | The secure environment provides at most limited opportunity for concealment of activity and for the storage of tools and other equipment |
| H16 | A secure environment remains such until all keys and other secret data stored in devices within the environment are destroyed or until all such devices are removed from the environment |

| No. | Security compliance statement |
|-----|--|
| H17 | <p>The secure environment contains either:</p> <ul style="list-style-type: none"> ▪ both the device and its host, and there are controls on the environment which prevent the device from being connected to any unauthorized device, and on the host to ensure that exhaustive attacks (on PINs), using legitimate function calls, are not feasible; or ▪ the device alone, which contains security mechanisms that protect against exhaustive attacks. |

8.1.9 PIN Security & TR39

The committee has mapped PIN Security and TR 39 requirements conclude that both standards are consistent. Refer to Appendix 1 SPVA Requirements Updated After PCI PTS v3. (April 2010) beginning on page 35 for a copy of this map. To facilitate the reading of this document, PIN Security Objectives definition will be used.

8.1.9.1 PIN Security

| No. | Security compliance statement |
|-----|--|
| 1 | PINs used in transactions governed by these requirements are processed using equipment and methodologies that ensure they are kept secure. |
| 3 | Keys are conveyed or transmitted in a secure manner. |
| 4 | Key loading to hosts and PIN entry devices is handled in a secure manner. |
| 5 | Keys are used in a manner that prevents or detects their unauthorized usage. |
| 6 | Keys are administered in a secure manner |
| 7 | Equipment used to process PINs and keys is managed in a secure manner |

8.2 Security Requirements Analysis

8.2.1 Security Requirements Standards Map

| PTS | ISO 13491:1 | ISO 13491:2 | PIN Security |
|-----------|-------------|-------------|--------------|
| F1 | | | |
| | | A41 | |
| F2 | | A32 | |
| | | A36 | |
| F3 | | A42 | |
| | 7.3.2 | A43 | 7 |
| | | A37 | 4 |
| | | A40/F9 | 4 |
| | | B20/E5 | 5 |
| | | B21 | 5 |
| | | E2/F3/F19 | 6/7 |
| | | E4 | 1 |
| | | F2 | 5/4/7 |
| | | F15 | 7 |
| | | F16 | 3/4 |
| | | F17 | 4 |
| | | F18 | 3 |
| | | F20 | 3/4 |
| | | F21 | 3/4 |
| | | F22 | 3 |
| | | G1 | 2 |
| G2 | 4 | | |
| H1... H22 | 7 | | |

9 Lifecycle Protection Methods

9.1 ISO 13491-1 Requirements

- During this phase, auditing and control procedures shall be implemented which have a high probability of preventing or detecting the unauthorized alteration of the device or the replacement of the device with a counterfeit substitute.
- Whichever method of key generation is used, key loading shall be performed in such a way that the secret or private key cannot be determined without collusion.
- Immediately prior to initial key loading, there shall be assurance that the device has not been subject to unauthorized modification or substitution. This may be accomplished by:
 - Testing and/or inspection of the device;
 - Auditing and control of the device post-manufacture, or subsequent to the most recent testing and/or inspection of the device;
 - Confirmation of the existence within the device of secret data by the manufacturer for the sole purpose of confirming the legitimacy of the device.
- Device management shall provide detection of theft or unauthorized removal of the device.

9.2 Protection Methods Analysis

Unlike ISO 13491-1, PTS does not make any distinctions between requirements and protection methods that may be used to protect the device during its lifecycle phases.

10 Audit and Control Principles

10.1 PTS

PED Security Requirements (managed by PCI SSC) are primarily concerned with device characteristics impacting the security of the PIN Entry Device used by the cardholder during a financial transaction. The requirements also include device management up to the point of initial key loading, but the evaluation process only addresses device characteristics.

The vendor is required to be compliant with the PTS management requirements, but the PTS does not define any Derived Test Requirement (DTR) for PD management requirements.

10.2 ISO 13491-1

ISO13491-1 proposes some recommendations to allow security stakeholders to cover the POS security audit and control in Post Manufacturing stage.

Auditing and control procedures shall be implemented which have a high probability of preventing or detecting the unauthorized alteration of the device or the replacement of the device with a counterfeit substitute.

And defines three evaluation methods: informal, semi-formal and formal.

- A risk assessment shall be undertaken as an aid in choosing which methodology is appropriate.
- Informal and semi-formal methods can use the checklists included in the ISO 13491-2.

| No. | Procedure | Post Manufacturing Stage |
|-----|---|--------------------------|
| 1 | One or more parties responsible for the device. | Mandatory |
| 2 | Careful screening of, or control over, personnel with access to a device designed for use in a controlled environment | Mandatory |
| 3 | Careful screening of, or control over, personnel with access to a device designed for use in a minimally controlled environment | Mandatory |
| 5 | Control mechanisms or sealing of the device in counterfeit resistant, tamper evident packaging to prevent undetected access to the device | Mandatory |
| 6 | Preparation and use of audit checklists | Mandatory |
| 7 | Verification that audit checklists are filled out accurately, on a timely basis, and by qualified personnel | Recommended |
| 8 | Key management procedures implemented as specified in the appropriate International Standard | Mandatory |

| No. | Procedure | Post Manufacturing Stage |
|-----|---|--------------------------|
| 9 | Accurate tracking of each device, by means of computerized or manually written records | Mandatory |
| 11 | Control of the distribution of device documentation | Recommended |
| 13 | Documented reporting procedures to cause timely detection of a device that has been removed without authorization from storage or from its operational location, or that has disappeared while in transit | Mandatory |
| 19 | Control over the maintenance process in order that the confidentiality of the device design characteristics is maintained | Mandatory / Recommended |

Secure environments: A secure environment provides an outer shell of protection around an insecure device and must be significantly more secure than a controlled environment. It can be a room designed and built for this specific purpose or it could be a safe or a secure cabinet. Whatever form the secure environment takes, only persons with authorized access to the device shall have access to the secure environment. A secure environment is often located within a controlled environment.

Controlled environments: A controlled environment is similar to normal computer rooms where there are access controls, allowing access only to authorized personnel. A controlled environment, however, has more stringent access controls and both its interior and the entrances are under surveillance.

Minimally controlled environments: These requirements aim to detect an attack, or theft, within a given maximum period of time.

Uncontrolled environments: There are no security requirements for uncontrolled environments.

10.3 ISO 13491-2

Annex A to H of this standard provides a checklist defining the minimum evaluation for use with all evaluations to assess the acceptability of cryptographic equipment.

11 Stakeholders

Vendors: PD vendors may be impacted by ensuring that the required mechanisms to provide security during this phase as defined in this document are implemented.

Manufacturers - EMS. (Electronic Manufacturing Services.): These companies may be impacted by supporting and deploying the security mechanisms as defined by PD Vendors in order to comply with the security requirements defined in this document.

Logistic Companies: These companies may be impacted by supporting and deploying the security mechanisms to guarantee the integrity and accountability of the PD during the storage and transport steps of this stage.

Key Injection Service Providers: These companies acting in behalf of acquirers may be impacted by supporting and deploying the security mechanisms to comply with the security requirements defined in this document for the key loading process.

Acquirers: These companies as the Key Scheme Authority may be impacted by supervising the Key Injection Service Providers observance of the security requirements defined in this document for the key loading process.

Auditors: These companies may be impacted in order to establish test plans according to SPVA recommendations and to audit any PD management activity performed by an actor who is interested in joining SPVA alliance.

12 SPVA Certification Requirements

12.1 SPVA Security Requirements

12.1.1 SPVA_Post_Manufacturing_Sec_Req_1

SPVA Requirements Definition: A security management system shall be defined and implemented for secure storage and transport activities.

SPVA Recommended Implementation: The security management system shall define the plans and procedures to enforce that the storage and transport activities are implemented in compliance with the ISO 28000:2007 Specification for security management systems for the supply chain.

12.1.2 SPVA_Post_Manufacturing_Sec_Req_2

SPVA Requirements Definition: Documented procedures exist and are followed to ensure that transfer of accountability for the device from the manufacturer to the initial-key-loading facility are completed.

There are four objectives under the accountability requirement:

- **Identification:** The process used to recognize an individual PD.
- **Authentication:** The process used to validate the claimed identity of the PD.
- **Non-repudiation:** The process of ensuring that a party in a dispute cannot or refute the validity of the assumption of a PD responsibility. (Ownership change.)
- **Lost detection and prevention.**
- **Traceability:** Audit information shall be selectively kept and protected so that actions affecting security can be traced to each PD.

SPVA Recommended Implementation: Accountable records shall be maintained that indicate the location and status of each device. The accountable party shall be identified by these records. When devices are transferred to another organization, another party becomes accountable for the devices. Therefore, the records at both the originating and receiving organization shall identify the devices and indicate the date of the transfer, the organization to/from which the transfer was made.

There shall be some means of confirming that accountability has been accepted by the receiving organization and the name of the party that is presently accountable for the transferred devices shall be included in the records of the transferring organization.

12.1.3 SPVA_Post_Manufacturing_Sec_Req_3

SPVA Requirements Definition: A secure mechanism that provides PD authentication shall be established during post-manufacturing processes.

SPVA Recommended Implementation: The PD authentication mechanism shall be based on an asymmetric key pair based on a Public Key Infrastructure. The PD manufacturer shall provide the appropriated information and security mechanism to validate the authenticity and integrity of the PD.

12.1.4 SPVA_Post_Manufacturing_Sec_Req_4

SPVA Requirements Definition: Documented procedures exist and are followed to implement and operate a Key Management Infrastructure to support the enforcement of key management practices for generation and/or acquisition, distribution, protection, and use (destruction) of keying material necessary to ensure the PD authenticity, integrity and (operability) under the Key Scheme Authority.

SPVA Recommended Implementation: The Key Management Infrastructure shall define the plans and procedures to enforce that the Key Management activities, specially the Key Loading process, are implemented in compliance with the ANSI X9 TR-39-2009 and PIN Security Requirements Version 2.0.

12.1.5 SPVA_Post_Manufacturing_Sec_Req_5

SPVA Requirements Definition: The organization shall establish, implement and maintain appropriate plans and procedures to identify and respond to security incidents.

SPVA Recommended Implementation: The plans and procedures shall define the steps that personnel shall use to ensure that security incidents are identified, contained, investigated, and remedied. The plans and procedures also shall provide a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs. Finally, the plans and procedures shall establish responsibility and accountability for all steps in the process of addressing security incidents.

The organization shall periodically review the effectiveness of its emergency preparedness, response and security recovery plans and procedures, in particular after the occurrence of incidents or emergency situations caused by security breaches and threats. The organization shall periodically test these plans and procedures wherever practicable.

12.1.6 SPVA_General_Req

SPVA Requirements Definition: Where an organization chooses to outsource any process that affects conformity with these requirements, the organization shall ensure that such

processes are controlled. The necessary controls and responsibilities of such outsourced processes shall be identified.

SPVA Recommended Implementation: The risks associated with outsourcing shall be managed through the imposition of suitable controls, comprising a combination of legal, physical, logical, procedural and managerial controls.

The organization shall periodically audit the outsourcer's compliance with the SPVA Security Requirements, or shall employ a mutually agreed independent third party auditor for this purpose.

12.2 SPVA Audit Control Objectives

12.2.1 SPVA_Post_Manufacturing_Aud_Req_1

SPVA Requirements Definition: The organization shall establish, implement and maintain a security audit program and shall insure that audits of the security system are carried out at planned intervals.

SPVA Recommended Implementation: The audit program, including any schedule, shall be based on the results of threat and risk assessments of the organization's activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results. Where possible, audits shall be conducted by personnel independent² of those having direct responsibility for the activity being examined.

The audit program shall include the following Audit criteria:

- The Audit criteria for PD storage and transport activities shall be at least in compliance with the ISO 28000:2007 Specification for security management systems for the supply chain.
- The Audit criteria for the Key Management processes shall be at least in compliance with X9 TR-39-2009 and PIN Security Requirements Version 2.0

² NOTE: The phrase "personnel independent" does not necessarily mean personnel external to the organization.

13 Rationale

13.1 SPVA Security Requirements Map

| SPVA | PTS | ISO 13491:1 | ISO 13491:2 | PIN Security |
|------------------------------|-----|-------------|-------------|--------------|
| Post_Manufacturing_Sec_Req_1 | F1 | | A41 | |
| Post_Manufacturing_Sec_Req_2 | F2 | | A32 A36 | |
| Post_Manufacturing_Sec_Req_3 | F3 | | A42 | |
| Post_Manufacturing_Sec_Req_4 | | 7.3.2 | A43 | 7 |
| Post_Manufacturing_Sec_Req_5 | | | A37 | 4 |
| | | | A40/F9 | 4 |
| | | | B20/E5 | 5 |
| | | | B21 | 5 |
| | | | E2/F3/F19 | 6/7 |
| | | | E4 | 1 |
| | | | F2 | 5/4/7 |
| | | | F15 | 7 |
| | | | F16 | 3/4 |
| | | | F17 | 4 |
| | | | F18 | 3 |
| | | | F20 | 3/4 |
| | | | F21 | 3/4 |
| | | | F22 | 3 |
| G1 | 2 | | | |
| G2 | 4 | | | |
| H1... H22 | 7 | | | |

13.2 SPVA Security Requirements Coverage

13.2.1 Secure Post-Manufacturing Processes

- Integrity: Covered by SPVA_Post_Manufacturing_Req_2.
- Accountability: Covered by SPVA_Post_Manufacturing_Req_2.

13.2.2 Initial Key Loading

- Confidentiality: Covered by SPVA_Post_Manufacturing_Req_4.
- Integrity: Covered by SPVA_Post_Manufacturing_Req_2, SPVA_Post_Manufacturing_Req_3 and SPVA_Post_Manufacturing_Req_4.
- Accountability: Covered by SPVA_Post_Manufacturing_Req_4 and SPVA_Post_Manufacturing_Req_4..
- Authenticity: Covered by SPVA_Post_Manufacturing_Req_3.
- Non-repudiation: Covered by SPVA_Post_Manufacturing_Req_4.

13.2.3 Secure Delivery and Storage

- Authenticity: Covered by SPVA_Post_Manufacturing_Req_1.
- Non-repudiation: Covered by SPVA_Post_Manufacturing_Req_1.

13.2.4 Incident Management

- Confidentiality: Covered by SPVA_Post_Manufacturing_Req_5.
- Integrity: Covered by SPVA_Post_Manufacturing_Req_5.
- Accountability: Covered by SPVA_Post_Manufacturing_Req_5.
- Authenticity: Covered by SPVA_Post_Manufacturing_Req_5.

13.2.5 SPVA AUDIT

- Preventing or detecting: SPVA_Post_Manufacturing_Aud_Req_1

13.3 SPVA Key loading Scenarios

There are two scenarios for key loading. In both scenarios the Initial Key is loaded at the point of manufacturing in compliance with requirement

SPVA_Post_Manufacturing_Sec_Req_4.

The two scenarios differ in the location the Customer keys are loaded. In the second scenario the Customer keys are loaded under the Customer's responsibility.

In both scenarios the Customer keys must be loaded in compliance with

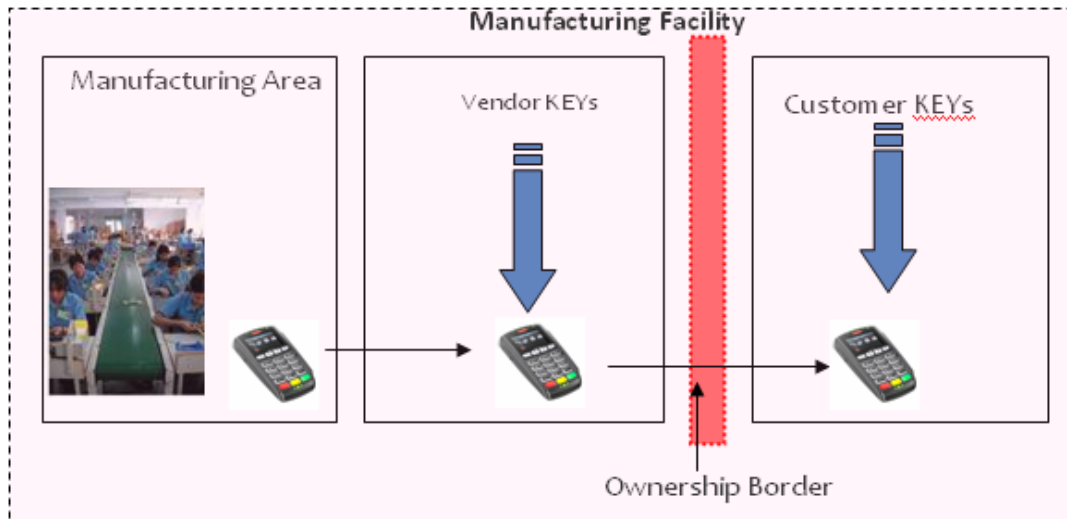
SPVA_Post_Manufacturing_Sec_Req_4.

For the second scenario, it is appropriate to discuss the key management process as being both necessary and sufficient. The Initial key is necessary to insure the integrity and authenticity of the PD during its complete lifecycle.

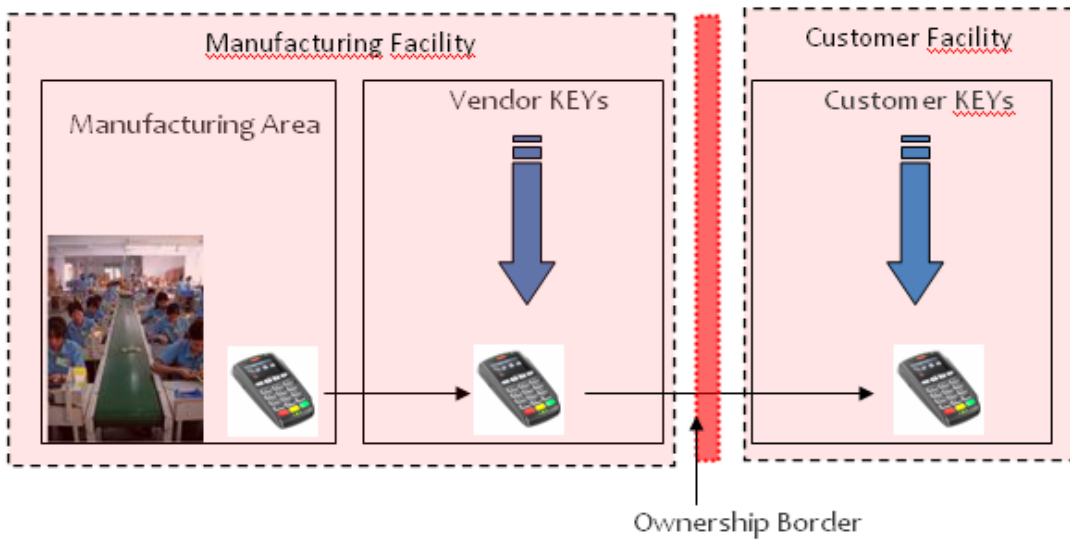
The PD manufacturer must provide the appropriated information and security mechanism to validate the authenticity and integrity of the PD.

Sufficiency is provided by allowing the Initial Key Facility to verify the PD authenticity and integrity based on the Vendor Keys before starting the Customer Key loading process.

1. Initial Key and second-tier key loaded at point of manufacturer



2. Initial Key loaded at point of manufacturer and second-tier key loaded at point of customer.



14 References

- PCI – PED Security Requirements Version 2.1. January 2009
- ISO 13491-1: 2007 Banking — Secure cryptographic devices (retail) — Concepts, requirements and evaluation methods
- ISO 13491-2: 2000 Banking — Security compliance checklists for devices used in magnetic stripe card systems.
- ISO 11568-1: 2005 - Banking — Key management (retail). Principles.
- ISO 11568-4:2007 - Banking -- Key management (retail) -- Part 4: Asymmetric cryptosystems -- Key management and lifecycle.
- ISO 11568-5: 2005 - Banking — Key management (retail) - Key lifecycle for public key cryptosystems.
- ISO IEC 11770-1: 1996 – Information technology – Security techniques - Key management - Part 1: Framework
- ISO IEC 11770-3: 1996 – Information technology – Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques.
- ISO 15782-1: 2003_Banking - Certificate Management – (Public Key Certificates)
- ISO 28000:2007 Specification for security management systems for the supply chain.
- ANS X9.42 - 1998, Public Key Cryptography for The Financial Service Industry.
- ANS X9.79-1:2001. Part 1: PKI Practices and Policy Framework.
- Payment Card Industry: PIN Security Requirements Version 2.0 January 2008. VISA
- PIN Security Program: Auditor’s Guide Version 2 January 2008. VISA
- Cryptographic Key Injection Facility: Auditor’s Guide Version 1.0 January 2008. VISA
- Payment Card Industry PIN Security Requirements March 2008. MasterCard.
- PCI PIN Security Requirements Version 2.0 January 2008. VISA
- ANSI X9 TR-39-2009. TG-3 Retail Financial Services Compliance Guideline Part 1:PIN Security and Key Management.
- CobIT 4.1 (Control Objectives for Information and related Technology). ISACA

15 Appendix 1 SPVA Requirements Updated After PCI PTS v3. (April 2010)

15.1 Introduction

The Payment Card Industry PIN Transaction Security (PTS) standard follows a defined 36-month lifecycle. The expiration of PCI PTS v 2.1 requirements date is defined by the PCI SSC, April 2011.

The PCI PTS Version 3.0 introduces significant changes in how PCI will be evaluating PIN acceptance on POI terminals. The PCI PTS Version 3.0 document is an evolution of the previous versions and supports a number of new features in the evaluation of POI devices.

The PCI PTS Version 3.0 document, like version 2.1 (January 2009), is only concerned with the device management for PIN-acceptance POI devices up to the point of initial key loading. Subsequent to receipt of the device at the initial key-loading facility, the acquiring financial institution and its agents (e.g., merchants and processors) are responsible for the device and are covered by the operating rules of the participating PCI payment brands and the *PCI PIN Security Requirements*.

15.2 PCI PTS v3 Requirements: Manufacturer and Initial Key Loading

| No. | Security compliance statement |
|-----|---|
| M1 | The device is shipped from the manufacturer's facility to the initial key-loading facility, and stored en route under auditable controls that can account for the location of every PED at every point in time. |
| M2 | Procedures are in place to transfer accountability for the device from the manufacturer to the initial key-loading facility. |
| M3 | While in transit from the manufacturer's facility to the initial key-loading facility, the device is: <ul style="list-style-type: none">▪ Shipped and stored in tamper-evident packaging; and/or▪ Shipped and stored containing a secret that is immediately and automatically erased if any physical or functional alteration to the device is attempted, that can be verified by the initial key-loading facility, but that cannot feasibly be determined by unauthorized personnel. |
| M4 | The development security documentation must provide the means to the initial key-loading facility to assure the authenticity of the TOE security relevant components. |
| M5 | If the manufacturer is in charge of initial key loading, then the manufacturer must verify the authenticity of the POI security-related components. |
| M6 | If the manufacturer is not in charge of initial key loading, the manufacturer must provide the means to the initial key-loading facility to assure the verification of the authenticity of the POI security-related components. |

| No. | Security compliance statement |
|-----|---|
| M7 | Each device shall have a unique visible identifier affixed to it. |
| M8 | <p>The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire lifecycle of the POI security-related components and of the manner in which those components are integrated into a single POI, e.g.:</p> <ul style="list-style-type: none"> ▪ Data on production and personalization ▪ Physical/chronological whereabouts ▪ Repair and maintenance ▪ Removal from operation ▪ Loss or theft |

15.3 SPVA Security Requirements Map

| PCI/PTS V.3 | PCI/PTS V.2 | SPVA |
|-------------|-------------|---|
| M1 | F1 | <u>Post_Manufacturing_Sec_Req_1</u> |
| M2 | F2 | <u>Post_Manufacturing_Sec_Req_2</u> |
| M3 | F3 | <u>Post_Manufacturing_Sec_Req_3</u> |
| M4 | - | <u>Post_Manufacturing_Sec_Req_3</u> |
| M5 | - | <u>Post_Manufacturing_Sec_Req_4 Scenario 1</u> |
| M6 | - | <u>Post_Manufacturing_Sec_Req_4 Scenario 2</u> |
| M7 | - | <u>Post_Manufacturing_Sec_Req_2 Redefinition required</u> |
| M8 | - | <u>New Requirement</u> |

15.4 SPVA Certification Requirements

15.4.1 SPVA_Post_Manufacturing_Sec_Req_2 (Redefined)

SPVA Requirements Definition: Documented procedures exist and are followed to ensure that transfer of accountability for the device from the manufacturer to the initial-key-loading facility is completed.

There are four objectives under the accountability requirement:

- **Identification:** The process used to recognize an individual PD. Each device shall have a unique visible identifier affixed to it.
- **Authentication:** The process used to validate the claimed identity of the PD.

- **Non-repudiation:** The process of ensuring that a party in a dispute cannot or refute the validity of the assumption of a PD responsibility. (Ownership change.)
- **Lost detection and prevention.**
- **Traceability:** Audit information must be selectively kept and protected so that actions affecting security can be traced to each every PD.

15.4.2 SPVA_Post_Manufacturing_Sec_Req_5 (New Requirement)

SPVA Requirements Definition (Same as PCI PTS v3): The vendor must maintain a manual that provides instructions for the operational management of the POI. This includes instructions for recording the entire lifecycle of the POI security-related components and the manner in which those components are integrated into a single POI, e.g.:

- Data on production and personalization
- Physical/chronological whereabouts
- Repair and maintenance
- Removal from operation
- Loss or theft

SPVA Recommended Implementation: Each PD vendor shall define a process to enforce this requirement. An audit and monitoring plan should be defined to obtain evidence that the process is followed as expected.