

Best Practices for Point of Sale Lifecycle Security

Minimum Security Recommendations



Produced by the ATMIA Debit Council
POS Industry Task Force, January 2007

Table of Contents

Foreword.....	4
Table of Acronyms.....	5
Chapter 1 What is Point of Sale (POS) Lifecycle Security?	7
Cardholder Security	8
POS Compliance Security	8
POS Deployment, Repair and Tracking Security	9
POS Physical Security.....	9
Pin & Encryption Security	10
POS Software Security	11
POS Connectivity Security.....	11
POS Decommissioning Security	11
Chapter 2 Top Tips for POS Cardholder Security	12
POS Customer Usage Guide.....	12
Top Five Tips for POS Transactions.....	14
Chapter 3 POS Compliance Security	15
Benefits of PCI DSS Compliance.....	15
PCI DSS	15
Compliance Validation and Payment Applications.....	17
The Principle of Safe Harbor.....	18
Chapter 4 POS Deployment, Repair & Tracking Security	19
Development Phase	20
Manufacturing Phase.....	21
Storage Phase	21
Key Loading Facility Phase	21
Merchant Use Phase	22
Decommissioning Phase	22
Repairs Phase	22
Chapter 5 POS Physical Security	23
Scope of POS Physical Security.....	23
Countertop POS	24
Portable POS.....	26
Handover POS.....	27
AFD (Automated Fuel Dispenser).....	28
Chapter 6 POS PIN & Encryption Security	30
Purpose of Recommendations.....	30
Objectives of PIN Security & Key Management.....	30
The Scope of PIN & Encryption Security Recommendations.....	31
PIN Security Recommendations	32
Key Management Recommendations.....	37
Specific Recommendations for Key Component Storage and Physical Access	44
Specific Recommendations for Key Loading and Entry.....	44
Specific Recommendations for Key Compromise and Destruction.....	46
Specific Recommendations for Key Equipment Management	48

Key Management Procedures	50
Guidelines for Key Management Procedures	51
Cryptography Best Practice Recommendations	51
Chapter 7 POS Software Security	53
The Role of POS Software.....	53
Processing POS Transactions using TCP/IP Over the Internet	53
Virtual Terminals.....	54
Tracer Programs.....	54
POS Software Development	55
Antivirus Software	55
Cryptography	56
Internet Protocols.....	57
Email.....	58
Remote Management	59
LAN Internet Protocols.....	59
Employees.....	60
Chapter 8 POS Connectivity Security	61
Cost Savings Bring Risk Too	61
What Can Go Wrong?	61
Documenting Your Network Connections is a Vital First Step	62
Dividing and Segmenting the Network is a Second Step	62
Selecting Critical Filtering and Access Controls the Third Step	63
Malicious Code Filtering	67
Outbound Filtering	67
Network Intrusion Prevention Systems	67
Securing Remote Access to the POS Network: The Fifth Step.....	69
Securing File Downloads	71
Chapter 9 POS Decommissioning Security	72
Introduction to POS Decommissioning & Disposal Recommendations	72
Resale of Equipment	72
POS Security Disposal Recommendations.....	73
POS Environmental Disposal Recommendations and Guidelines	73
Relevant References	75
Acknowledgments	77
Disclaimer.....	78

Foreword

This Best Practices Manual for Point of Sale (POS) Lifecycle Security sets out to provide minimum international security guidelines focused on maintaining a trusted environment for POS transactions.

The automation of credit and debit card transactions at the point of sale has been growing in scale since the early 1980s. With the growing proliferation of new ways to use a card (for example, electronic commerce, mobile commerce, mobile phone top up etc), new card types like pre-paid cards and new technologies such as smartcards, the maintenance and implementation of security standards in financial services has become ever more onerous and complicated.

In addition to all this change, there is the growing problem of migration of fraud in multiple directions – geographically, across countries, vertically, across the lifecycle of delivery channels, and horizontally, across different channels (for example, from compromises of cards and PINs through phishing, to ATM fraud or from POS compromises to ATM fraud).

At the beginning of 2006, the ATMIA Debit Council set up a POS industry task force. Its aim was to help prevent POS fraud through security best practice recommendations for the POS lifecycle. In addition, it wanted to facilitate closer collaboration between the POS and ATM industry to jointly fight debit card fraud.

This best practice manual is the result. We trust it will lead to a greater understanding of POS lifecycle security and to greater industry collaboration in the fight against fraud. This manual is intended for several audiences:

- Retailers
- POS processors
- Encryption Service Organizations
- Auditors, Security personnel
- Managers who have responsibility for securing their POS installations and for meeting network and PCI requirements

It is anticipated that later versions of this manual will discuss security practices for RFID POS devices and add a comprehensive Glossary of Terms for POS security.

The POS Security Task Force
ATMIA Debit Council
January 2007

TABLE OF ACRONYMS

Acronym	Meaning
ANSI	American National Standards Institute
ATM	Automated Teller Machine
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DSE	Data Storage Entities
DUKPT	Derived Unique Key Per Transaction
ECB	Electronic Code Book
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EPROM	Erasable Programmable Read-Only Memory
HSM	Host Security Module or Hardware Security Module
ISO	International Organization for Standardization
JCB	The Japan Credit Bureau
KEK	Key Encrypting Key
PCI DSS	The Payment Card Industry Data Security Standard
PCI PABP	Payment Card Industry Payment Application Best Practices
PED	Pin Entry Device
PIB	PIN Block
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POP3	Post Office Protocol version 3
POS	Point of Sale
PROM	Programmable Read-Only Module
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer

TESM	Tamper-Evident Security Module
TMK	Terminal Master Key
TPP	Third Party Processors
TRIPLE DES (3 DES)	The newest encryption standard being adopted by the car payment industry as a proactive measure against potential attacks to “crack” standard DES keys. 3DES involves DES encryption of each data block three times with different keys, using three successive iterations of the DES algorithm. It can use either a 128-bit (16-byte) or 192-bit (24 byte) key. The 3DES standard is endorsed by both the ISO and ANSI committees.
TRSM	Tamper-Resistant Security Module
ZMK	Zone Master Key
ZPK	Zone PIN Key

CHAPTER 1

WHAT IS POINT OF SALE (POS) LIFECYCLE SECURITY?

In the field of security, the saying “a chain is only as strong as its weakest link” is especially true. Criminals are known to migrate along the path of least resistance to the softest, or least risky, target. Any security system is only as strong as its weakest link.

When it comes to the security of the millions of point of sale (POS) devices in operation today, it is essential to define the operational lifecycle of these terminals. Defining the lifecycle helps to highlight the points at which criminals can attack POS devices.

Once the POS lifecycle has been described and defined, security best practices can be directed at all operational phases so that the whole “chain” is strong and secure.

The objective of lifecycle security best practices is to maintain a trusted environment for POS transactions. *It is essential for all stakeholders in the POS security lifecycle to have **written** procedures to ensure that proper processes are consistently followed, and that they stress the principles of dual control and split knowledge¹ to protect the encryption key.*

In biology, lifecycle refers to the complete series of stages through which an organism passes from conception, through maturation to eventual death. The idea of a lifecycle is that these stages are linked as the organism passes from one stage to the next in a natural sequence. The POS operational lifecycle covers all the phases, processes, systems, procedures, and operations required to deliver POS services to bank customers and cardholders.

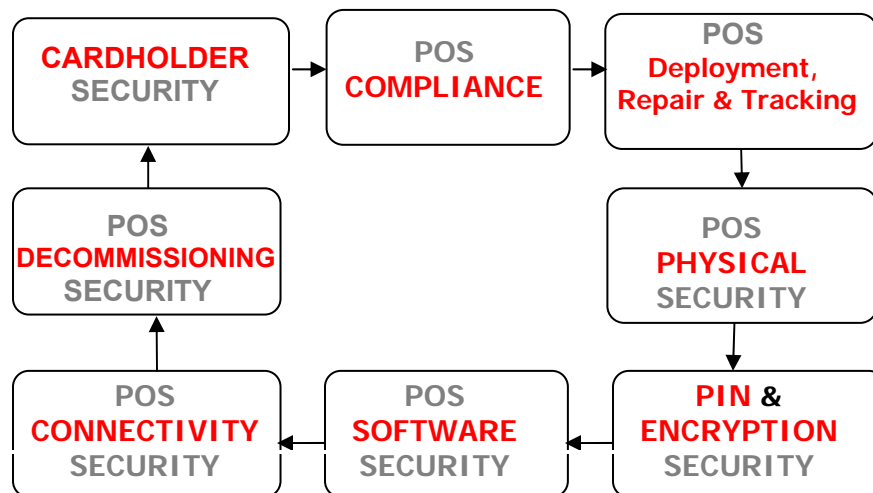
The term POS lifecycle refers to all the interlinked phases involved within the business processes required for the functioning and operating of the POS. In the POS business or operational lifecycle, certain processes, actions, and operations happen in a sequence of steps resulting in POS devices carrying out electronic transactions for cardholders. For example, for the POS device to effect an electronic payment, the cardholder needs to insert his card and identify himself (for example, through a PIN or signature). Then, the transaction needs to be authorized by his bank through a process that links the payments terminal via a network and switches to the bank’s authorizing system.

¹ Dual Control means that at least two authorized individuals are required to work in partnership to carry out an activity, such as generating, storing, or loading the clear text components of a key. Split Knowledge means that no single individual knows, or has access to, a whole entity, be it all the clear-text components of a key, or the combination of a safe where key components are stored.

When applied to POS security, this business lifecycle is seen as a series of phases where different kinds of protection are needed at different points along the lifecycle. Lifecycle security is the strategy of looking in a high-level, coordinated way, at all the phases along the lifecycle, constantly assessing crime migration patterns. Criminals are quick to spot vulnerabilities and gaps in the lifecycle.

Figure 1: Protecting the POS Lifecycle

Protecting the POS Lifecycle



Cardholder Security

Cardholder security refers to the ways in which cardholders can be educated to manage their card and POS usage in a sensible and security-conscious way. The industry should educate cardholders to be co-managers of their bank accounts, finances and cards. Law enforcement agencies agree that increasing cardholder security awareness can lead to significant reduction in fraud.

POS Compliance Security

These best practices are intended to ensure the following:

- That the POS device has been tested and that it is an approved Tamper-Resistant Security Module (TRSM) (approved as a TRSM, that is, by the network or PCI standards company)
- That the device has been inspected for tampering before the encryption keys are injected

- That either a DUKPT or Triple DES key that was created under the principles of dual control and split knowledge² has been injected into the device before PINs are entered
- That each device will have unique keys

POS Deployment, Repair and Tracking Security

These best practices will cover terminal inventory and tracking controls during all phases of its lifecycle:

- During the manufacturing phase
- While in transit and during testing
- During the key injection process and the installation commissioning process
- During operation (merchant use phase)
- During offline periods of storage, repair or inactivity

During each phase, it is important to track the movements of the device including which individuals have access to the device from the time of manufacture and key injection to the time of approval and installation. The purpose here is to control the device so that it cannot be intercepted and illegally modified. Once the device arrives at the retailer, it needs to be securely initialized to complete the deployment phase. It is critical that physical access and monitoring controls exist at the manufacturer, repair facility, injection facility, storage site, and retailer to reduce the risk of interception and the surreptitious insertion of a parasite or monitoring device.

POS Physical Security

POS physical security covers the security measures undertaken to ensure that the POS machine is properly installed, managed, and protected in a way that addresses and manages risks of attacks against it. These security measures manage and protect against theft and illegal modification. These measures also protect the cardholder's PIN entry privacy. POS devices should be inventoried and placed in secured, locked and monitored areas during storage, servicing and shipping. Physical security measures can encompass heavy duty "potting" or binding of the device to the logic unit. It can also encompass additional bolting, straps or other measures which would impede the removal of a device once it is operational.

² Dual Control means that at least two authorized individuals are required to work in partnership to carry out an activity, such as generating, storing, or loading the clear text components of a key. Split Knowledge means that no single individual knows, or has access to, a whole entity, be it all the clear-text components of a key, or the combination of a safe where key components are stored.

PIN & Encryption Security

The move to PIN entry as a form of cardholder verification at the point of sale demands that PINs and customer PIN entry be protected to the same standard as those in ATMs. Additional controls should be introduced to address differing needs for physical security at each terminal. For example, attackers could capture a PIN and the magnetic stripe data and create a counterfeit magnetic stripe card that could be used at other terminals such as ATMs. If PIN Entry Devices (PEDs) are shown to be insecure, cardholders will cease using their PINs, thus negating the additional level of security that PIN authorization gives to a transaction.

Cryptographic security has to do with the protection of PIN numbers, utilizing secure encryption key management policies and procedures based on ANSI X9.8 and X9.24. Cryptography, along with strong encryption key management, is used to protect PINs and PIN keys to reduce the risk of financial loss by fraud, thereby maintaining the integrity and confidentiality of the PIN debit network and instilling cardholder confidence in the use of both the ATM and the POS networks. The logical units which form POS or EPOS terminals can be implemented in a variety of physical configurations and the requirements for PIN encryption and authentication vary according to this configuration.

Protecting the card data and the means of customer identification from potential compromise is vital for the security of all delivery channels, whether the delivery channel be PIN, signature, or password. Additionally, all the other card transaction data carried within the transaction message from the POS terminal and through the authorization process needs to be protected from potential interception and misuse. This can be accomplished in real-time capture messages with the use of transaction keys for selective encryption and for authentication of messages. However, cryptographic security systems may also be used in a non real-time capture message environment.

Note that the card schemes have requirements regarding the security and storage of data.

POS transactional and data security is about initiating, implementing, and maintaining information security within payment networks. As messages and transactions in these networks contain both sensitive cardholder data and related financial information, it is important that the networks safeguard this information. The transactional security controls should be applied throughout a POS payment network, from the POS to the authorization process, including all transaction processing and the generation and storage of PINs and cryptographic keys.

POS Software Security

These best practices will cover the prevention of PINs and track 2 data from being stored on the POS software. POS software security also refers to general cyber security for computer, network, and information security as well as guidelines for operating POS platforms. The logical functions may either be in devices located at the point of sale or may be included in software running at the outlet or a central computer fronting several outlets. These systems may be bank owned or card acceptor owned.

POS Connectivity Security

POS Connectivity Security involves line encryption and protection of data over the communications lines between POS devices and their host systems to prevent interceptions of data through devices like wire-tapping or “wireless” tapping.

POS Decommissioning Security

POS decommissioning security involves ensuring that POS management entities have policies and procedures in place to ensure that POS devices due for decommissioning have their cryptographic keys safely removed when the terminal is de-installed and that the device is then “zeroized”. “Zeroized” devices have no remaining encryption keys or data within them. Procedures should exist and should be followed during the physical removal and transportation of the de-installed device to ensure that it cannot be stolen, intercepted or otherwise acquired by fraudsters or criminals with a view to illegal “reverse engineering” in unauthorized modifications or through obtaining key material which can compromise PINs.

CHAPTER 2

TOP TIPS FOR POS CARDHOLDER SECURITY

POS Customer Usage Guide

The following Point of Sale Customer Usage Guide is offered to enhance the security of the POS customer experience. Cardholders are sometimes in a position to avoid common POS crimes. These tips will help them to understand what they can do to avoid becoming victims of some POS crimes.

Check the Area around the POS Device

- Scan the area briefly as you approach the cashier to ensure no electronic surveillance cameras are directed towards the POS device. Notify a manager if there are any suspicious-looking individuals around. Avoid using the terminal if you feel unsafe, if it looks unusual, such as having strange labels on it, or if it looks like it has been tampered with.
- Avoid opening your purse, bag, or wallet while you wait in line. Rather have your card ready in your hand *before* you approach the point of sale.

Stay Focused During Transaction

- Be especially cautious if strangers offer to help you complete the transaction, even if you are experiencing difficulty with it. Never allow anyone to distract you while you are at the point of sale. If the cashier or retail clerk offers to “help” you by entering your PIN or removing the card from your sight, kindly refuse the offer.
- Ensure your handbag, wallet, and/or possessions are secure if and when you are asked to sign the transaction slip.
- Be aware of other customers trying to observe your transaction or standing too close to you. Check that other individuals in the line keep an acceptable distance from you.
- Be on the look out for individuals who might be watching you enter your PIN. If necessary, obstruct unauthorized viewing of your PIN while it is being entered. Do this by raising your hand for cover or by positioning yourself so that it is difficult for others to see you enter your PIN.
- If there is a delay, timeout, or cancelled or aborted transactions, and if a second attempt is made to complete the transaction, make note of the date and location and check your monthly statement to ensure a double debit has not occurred.

- If you notice unusual messages on the terminal screen or if you are prompted to enter your PIN twice, be sure to notify store personnel or the retailer's customer service department. You should only have to enter your PIN once for the transaction.
- If you requested cash back on the POS transaction, make sure you receive the cash and check the amount on the transaction slip.
- Never let your card out of your sight during a transaction and follow the merchant, retailer, or waiter if they move away to another area to swipe your card. The merchant should only run the card through the POS terminal, not through any other device.
- Do not be in a hurry during the transaction, and carefully secure your card and/or cash in your wallet, handbag, or pocket *before* leaving the counter. Do not forget to take your card with you!

Protect your PIN, Card, and Account

- Do not be tricked into providing the three digit or four digit security codes that appear on the front or back of your card, not even to the bank, cashier, or police (*except in cases of card transactions with **reputable** companies with whom you feel comfortable, phone orders, and Internet-based payments*). These codes are intended to prevent thieves from copying your card.
- Do not give your card or PIN number to any stranger. Memorize your PIN (if you must write it down, do so in a disguised manner and never carry it with your card). Try not to use obvious and guessable numbers for your PIN like your date of birth. Please remember financial institutions **NEVER** use email, telephone, or other means to ask you for your PIN.
- If your card gets retained or lost or if you are interfered with at a point of sale, report this immediately to the bank and/or police.
- Keep your printed transaction record so that when you receive your monthly statement, you can check that the correct amounts were debited from your account.

Top Five Tips for POS Transactions

To enhance the security of the POS customer experience

1. Feel physically secure by ensuring there are no cameras around, no one suspicious is nearby, and no one is able to peek over your shoulder while you enter your PIN. Notify a manager if anything appears unusual or unsafe.
2. Secure your possessions (purse, bag, wallet, card, and money) before, during, and after the transaction. Don't hurry unnecessarily.
3. Have your card in hand when approaching the POS device, and shield your hand when entering your PIN.
4. Enter your PIN only once. Do not tell anyone what your PIN number is, not even the bank, cashier, or police.
5. Always maintain possession of your card except when the teller or cashier is using it to process your transaction.

CHAPTER 3

POS COMPLIANCE SECURITY

These best practices are intended to ensure the following:

- That the POS device has been tested and that it is an approved Tamper-Resistant Security Module (TRSM) (approved as a TRSM, that is, by the network or PCI standards company)
- That the device has been inspected for tampering before the encryption keys are injected
- That either a DUKPT or Triple DES key that was created under the principles of dual control and split knowledge has been injected into the device before PINs are entered
- That each device will have unique keys

The ATMIA Debit Council regards the requirements of The Payment Card Industry Data Security Standard (PCI DSS) as binding on the industry. **The principles of dual control and split knowledge³ are fundamental to the protection of encryption keys. These principles should be applied throughout all key lifecycle stages and included in relevant written procedures.**

Benefits of PCI DSS Compliance

Benefits of compliance include limiting financial and reputational risk, protecting the consumer, and promoting confidence in the payment industry.

PCI DSS

PCI DSS resulted from collaboration between MasterCard Worldwide and Visa International to create common industry security requirements. PCI DSS was subsequently adopted by American Express, Discover Financial Services, and The Japan Credit Bureau (JCB). These electronic payment networks collectively founded the PCI Security Standards Council (www.pcisecuritystandards.org) and published the standard.

³Dual Control means that at least two authorized individuals are required to work in partnership to carry out an activity, such as generating, storing, or loading the clear text components of a key. Split Knowledge means that no single individual knows, or has access to, a whole entity, be it all the clear-text components of a key, or the combination of a safe where key components are stored.

Twelve PCI DSS Requirements in Six Categories

1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

2. Protect Cardholder Data

Requirement 3: Protect stored data

Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update antivirus software

Requirement 6: Develop and maintain secure systems and applications

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

Compliance Validation and Payment Applications

In addition to the twelve compliance requirements for the PCI DSS, there is validation of compliance whereby entities verify and demonstrate their compliance status to an independent assessor. The independent assessor provides a report to the merchant, switch or processor. Upon clearance of any open issues (cited by the independent assessor that may be a bar to full or nominal compliance) the independent assessor notifies the network that the entity is PCI compliant. The network, e.g. Visa, will then place the entity on its web-based approval list.

Acquirers are responsible for ensuring that all of their merchants comply with the PCI DSS requirements. However, each network has defined 'Merchant Levels' based on the type and volume of transaction. Service providers are classified as either Third-Party Processors (TPP) or Data Storage Entities (DSE). They are required to be PCI DSS compliant as are issuers and acquirers, who in turn, are responsible for ensuring that the merchants are in compliance.

Although there may not be a direct contractual relationship between merchant service providers and acquirers, card associations define which members are responsible for any liability that results from non-compliance. Each association has guidelines and best practice recommendations for payment application vendors and software developers.

Merchants and service providers need to take immediate action in case of a suspected or confirmed security breach. Compromised entities should take the following actions, which should be contained in written procedures:

1. Once the compromise has been identified take the appropriate measures to contain and limit the exposure.
2. Compromised systems need to be identified and isolated, but they should not be accessed.
3. Document and log all actions taken.
4. All forensic evidence, such as computer logs, need to be secured and preserved.
5. Wireless networks should change the Service Set Identifier (SSID – a value which is broadcast to anyone who wishes to log on) on their connected systems, except for the compromised systems.
6. Alert all necessary parties including internal security, the association fraud group, the merchant bank if applicable, and the appropriate law enforcement agencies.
7. Provide the compromised accounts to the associations in a secure manner.
8. Provide the associations with incident reports, and follow other procedures depending on the type of compromise and level.

The Principle of Safe Harbor

Safe Harbor provides members in networks that follow PCI protection from fines and compliance exposure in the event its merchant or service provider experiences a data compromise.

To attain Safe Harbor status a member, merchant, or service provider must maintain full compliance at all times, including at the time of breach. A forensic investigation will be performed and a member must demonstrate that prior to the compromise their merchant had already met the compliance validation requirements and demonstrated full compliance. Submission of compliance documentation does not necessarily provide the association members Safe Harbor status. The entity must have complied with all the requirements at the time of the compromise.

CHAPTER 4

POS DEPLOYMENT, REPAIR & TRACKING SECURITY

There have been reports of POS systems being compromised in the field during normal operation sometime after deployment. These devices are modified in such a way that cardholder information, like the magnetic stripe data and the PIN, is recorded. The recorded data is then used to commit fraud in a variety of ways, including cash withdrawals from ATMs.

In response to this threat, POS payment security is being strengthened. It is becoming more and more difficult to modify payment systems after they have been deployed by using tamper evidence and tamper resistant methods to detect unauthorized modifications. As has been mentioned, a security system is only as strong as its weakest link. As the security of the device improves, the vulnerability is shifting such that the unauthorized modifications may be easier to make before deployment.

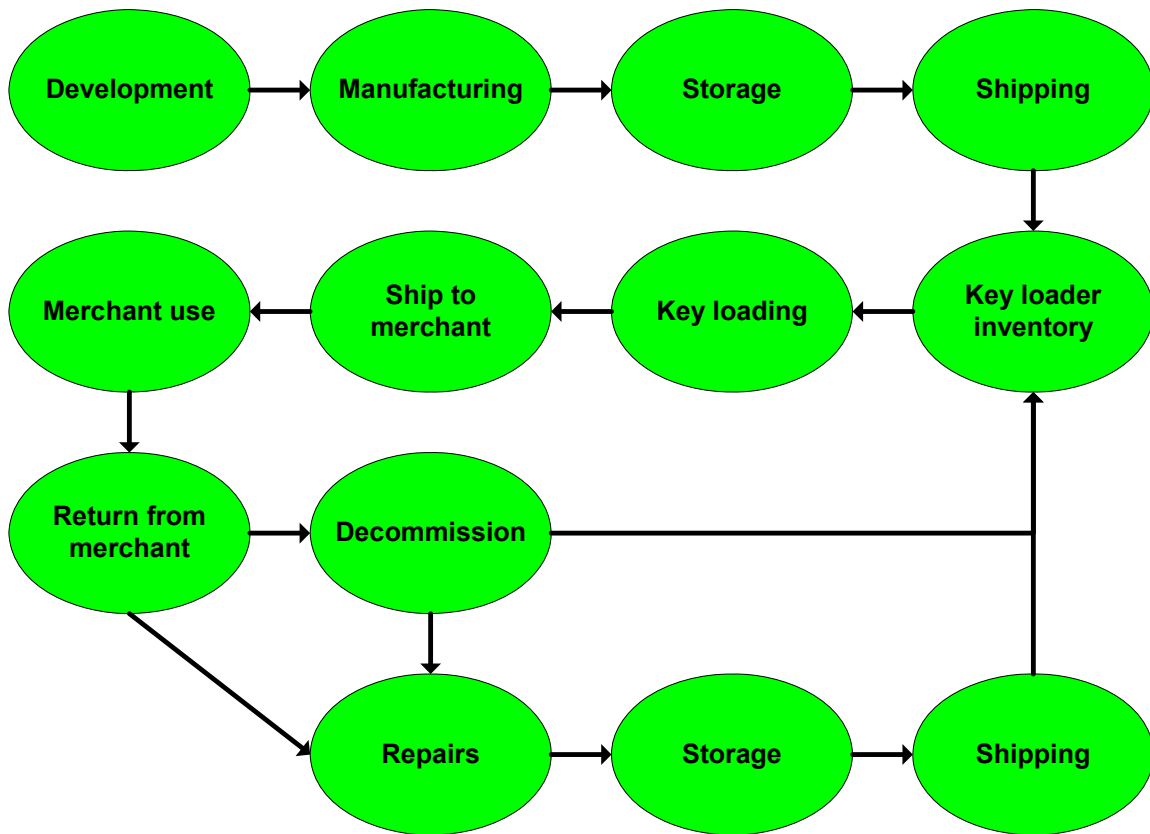
The best practices in this chapter will cover terminal inventory and tracking controls during all phases of its lifecycle:

- During the manufacturing phase
- While in transit and during testing
- During the key injection process and the installation commissioning process
- During operation (merchant use phase)
- During offline periods of storage, repair, or inactivity

The security measures required to protect the POS system prior to deployment will vary based on the security design of the device. These security measures must be established so that unauthorized modifications are not made to the device before it is deployed. This enables the cardholder's information to be recorded securely when the POS system is deployed.

The illustration below is the lifecycle of a PIN Entry Device (PED). The security guidelines for PEDs are a good foundation for security implementation in *any POS system*. Each phase of the PED lifecycle is discussed along with any applicable standards or testing programs for each phase.

Figure 2: PED Lifecycle



PED Development Phase

Security must be designed into a product at the earliest stages of development. It is extremely difficult to significantly increase the physical security after a product has been developed. Therefore, the level of security is established in the initial design.

Check the ISO requirements defined in Chapter 6 “POS PIN & Encryption Security” in the sections “Recommendations for TRSMs” and “Recommendations for PEDs”.

Security guidelines include:

- Perform due diligence when selecting logical modules or determining secure components
- Test for vulnerabilities including side channel attacks (examples include Simple Power Analysis and Differential Power Analysis)
- Submit products for security review by an independent assessor (for example, PCI PED program)

PED Manufacturing Phase

Most manufacturing facilities follow very precise procedures when building products. The products are defined by a bill of materials and specific build instructions. Products are inspected at several steps in the manufacturing process. Inventory controls are in place and access to components is limited.

Security guidelines during the manufacturing phase are:

- Ensure product is built to the bill of materials
- Physical security measures can encompass heavy duty “potting” or binding of the device to the logic unit. It can also encompass additional bolting, straps or other measures which would impede the removal of a device (once it is operational)
- Ensure firmware has not been modified

PED Storage Phase

PEDs must be securely stored to prevent undetected and unauthorized modifications to the device. PEDs could be stored at a variety of places during their lifecycle up to de-commissioning. The storage requirements will vary depending on the design of the device. Two methods of storage are:

1. A secure storage facility with dual access control so that one person is never alone in the storage area
2. Tamper resistant or evident packaging

Some devices may be secured during the manufacturing process; therefore, they would not require additional secure storage.

At this phase of the device’s lifecycle, it needs to be protected from unauthorized modifications before being deployed. A secure storage area must physically protect the device so that no one person can gain access. When relying on tamper evidence, either with tamper-evident packaging or a tamper-evident device design, tampering must be detected prior to loading keys into the device. Any tampering must be investigated to ensure there have been no unauthorized alterations of the device.

PED Key Loading Facility Phase

The key loading facility must also store the device in a secure manner as described in the above storage section. Processes and procedures are followed to ensure the overall secure handling of the device. Key loading facilities should be inspected to ensure that devices are not tampered with and that keys are handled in a compliant manner. Physical access to the facility should be limited by secure access or similar means. Devices must be inspected by the key loader for any signs of tampering prior to key injection. It is critical that software not be used to manage or load the keys, create variants, or translate pins.

PED Merchant Use Phase

Merchant use is the longest part of the device's lifecycle. This is the time the device is most vulnerable to attack. The security of the system must rely on the physical and logical security of the device as it is in operation.

The merchant should have written procedures to follow during this phase. Merchant verification should be emphasized in these procedures. The merchant should have a contact phone number of the PED supplier/operator responsible for maintaining it. This number should be available to the merchant at the PED device. When a person comes to upgrade or substitute or maintain the PED in any way, the merchant should call the phone number to verify authenticity of the repairman/installer, i.e. determine authorization for the PED repair, upgrade, or substitution. The merchant should verify the repairman's picture identification, log both the visit and repairman's identification, and, if possible, notify the repairman that the visit is being recorded by a security camera. If the visit is during non-business hours, the merchant should verify authorization of the repair with the PED supplier/operator on the following business day.

PED Decommissioning Phase

When a device is returned from its operational environment, it must be decommissioned (see Chapter 9 "POS Decommissioning Security"). At a minimum, the encryption keys must be cleared from the device. The method to clear the keys will vary depending on the design of the device. Once the keys have been cleared the device must be securely stored like in the manufacturing phase. If the device is to be re-deployed, it should be thoroughly inspected to ensure it does not have any unauthorized modifications.

PED Repairs Phase

The repairs phase is very similar to the manufacturing phase. In both phases the facility has all the parts to produce a working device. They also carry all the parts that could be used to conceal tamper evidence in the case of unauthorized modifications. A concern in the repair phase is that the repair facility is typically not the original manufacturer. The product, after repair, still carries the name and brand of the original manufacturer, so unauthorized modifications can reflect poorly on the original manufacturer. It is therefore recommended that the merchant should contact the manufacturer to notify them of any repairs due to be carried out by a third-party.

Bills of material must be up-to-date and firmware must be up-to-date. In addition, only authorized components should be used. Firmware is the logic or commands that are embedded inside the hardware module.

CHAPTER 5

POS PHYSICAL SECURITY

Scope of POS Physical Security

The POS device provides the interface between the merchant's customer, with their debit card, and the retail banking system that processes the transaction. There are tens of millions of POS PIN entry devices worldwide that facilitate purchase transactions at such diverse sites as convenience stores, petrol stations, multi-lane retail stores, small merchants, taxi and limousine services, and other point-of-purchase options.

Different POS operating environments are described as one or more of the following:

- Countertop
- Portable
- Handover
 - PIN entry only
 - Customer-activated with PIN entry
- AFD (Automated Fuel Dispenser)

In this chapter, the POS operating environment is defined along with a description of the scope of security. The possible observation corridors will be identified. This is followed by suggestions for physically securing the POS operating environment. The environment can and should be secured in the following instances:

- Choosing and maintaining a secure location site (site security)
- Installing the device
- Inspecting the device
- Suspected fraud response

Table 1: Maintaining Physical Security

POS Operating Environment	Checkpoints for maintaining physical security		
	Location Site Security	Installing Process	Inspection Process
Countertop	✓	✓	✓
Portable			✓
Handover	✓		✓
AFD	✓	✓	✓

Countertop POS

Definition of Countertop POS

Countertop POS devices may be fixed to a countertop, usually on a permanent stand, or somewhat unfixed depending on the merchant and installation choice. In both cases the countertop POS device is co-located with the cash register or point-of-purchase. Typically, POS devices are situated in places like convenience stores, petrol stations, supermarkets, and shopping malls.

Scope of Security for Countertop Devices

In a countertop environment, the POS device is almost always within view of the merchant. Unlike portable devices, removal of the POS device is unusual; and removal would make the integrity of the POS device suspect. The scope of security then makes certain presumptions that limit risk:

- The POS device stays within the merchant's environment
- The merchant environment precludes unattended operation
- Some degree of surveillance usually augments human presence
- The POS device is typically co-located with the point-of-purchase (for example, cash register)

Observation Corridors

Observation corridors occur when people or observation devices (for example, security cameras) can view the POS operating system. Observation corridors weaken the security of the POS operating environment.

- Clerk or merchant looking over keypad when POS device is customer facing
- “Shoulder surfing” (when a person peers or peeks over another’s shoulder to watch or spy on them) from other customers in the queue
- Malicious observation from security cameras
- Observation by means of safety mirrors

Site Security

The location of the POS device should be assessed in terms of the presence of video cameras, relative position of other customers, and orientation relative to the clerk. Video cameras should be deployed to observe the device, but not the keypad. The customer should be able to position themselves between the POS device and other customers. Since the customer cannot effectively block observation by the clerk, consideration should be given to enhancing the area surrounding the POS device with visual barriers.

A written assessment should be produced for the merchant and installer that identifies the potential vulnerabilities, proposed remedies, and installation guidelines.

Installation Process

It is preferred that the POS device be mounted to a sturdy metal stand that will allow some variation in positioning. The ability to position the POS device enhances customer security. The metal stand should be securely attached to the countertop surface with hardware that prevents easy removal (for example, carriage bolts). If the POS device does not incorporate a privacy shield, installation should include placing visual barriers to prevent PIN observation by other customers or the clerk.

Inspection Process

The merchant should periodically inspect the POS device for evidence of physical penetration. Such penetration may be disguised under new or refurbished labels. The device should be examined along case seams and connector ports for evidence of wires exiting the unit. If compromise is suspected, the merchant should contact the installer or processor representative.

Portable POS

Definition of Portable POS

A portable POS environment exists when the merchant or clerk transports the POS device to the point of service. Typical uses are in food delivery and rental drop-off. In some cases the device is retained by the clerk or merchant for card swiping/insertion and then passed to the customer for PIN entry. Alternatively, the device may be customer-activated where the customer swipes/inserts their card and enters the PIN number. In this sense portable POS devices share similar security concerns with handover POS devices.

Scope of Security for Portable Devices

In a portable environment, the POS device is almost always within the view of either the merchant or customer (at transaction time). Both the clerk and customer can avail themselves of gross physical inspection of the POS device. The scope of security then makes certain presumptions that limit risk:

- The POS device stays within the merchant's control
- The merchant environment precludes unattended operation

Risk increases, however, because prolonged absence from service is not easily detected. This risk is addressed by the tamper mechanisms of the device itself; thus, outside the scope of this chapter.

Observation Corridors

- Clerk or merchant looking over keypad when POS device is customer-facing
- "Shoulder surfing" from other people standing nearby (for example, airport rental car, carnivals, flea markets, and fairs)

Inspection Process

The merchant should periodically inspect the POS device for evidence of physical penetration. Such penetration may be disguised under new or refurbished labels. The device should be examined along case seams and connector ports for evidence of wires exiting the unit. If compromise is suspected, the merchant should contact the installer or processor representative.

Handover POS

Definition of Handover POS

Handover POS devices may be either PIN-entry only or customer-activated. In both cases the handover POS device is co-located with the cash register or point-of-purchase and is either customer-facing or passed from the merchant to customer. Customer-facing devices might be in a cradle. Typically, they are situated in convenience stores and small merchants.

Scope of Security for Handover Devices

In a handover environment, the POS device is almost always within the view of either the merchant or a customer. Unlike portable devices, removal of the POS device is unusual and would make the integrity of the POS device suspect. The scope of security then makes certain presumptions that limit risk:

- The POS device stays within the merchant's environment
- The merchant environment precludes unattended operation
- Some degree of surveillance usually augments human presence
- The POS device is typically co-located with the point-of-purchase (for example, cash register)

Observation Corridors

- "Shoulder surfing" from other customers in the queue
- Malicious observation from security cameras
- Observation by means of safety mirrors

Site Security

The location of the POS device should be assessed in terms of the presence of video cameras, relative position of other customers, and orientation relative to the clerk. Video cameras should be deployed to observe the device but not the keypad. The customer should be able to position themselves between the POS device and other customers — typically the customer uses their body to obscure covert surveillance.

A written assessment should be produced for the merchant and installer that identifies the potential vulnerabilities, proposed remedies, and installation guidelines.

Inspection Process

The merchant should periodically inspect the POS device for evidence of physical penetration. Such penetration may be disguised under new or refurbished labels. The device should be examined along case seams and connector ports for evidence of wires exiting the unit. Since this is a portable device, evidence of external wires is likely an antenna. If compromise is suspected, the merchant should contact the installer or processor representative.

AFD (Automated Fuel Dispenser)

Definition of an AFD

AFD devices may be fixed to a structural pole or incorporated into a fuel pump. The latter case is often called “pay at the pump.” In the former method, the AFD is a component of a system that accepts cash or cards and requires identifying the pump to be dispensed.

Scope of Security for AFDs

Whether the AFD is pay at the pump or incorporated into the system, device is not within view of the merchant unless it is by surveillance cameras — itself a security concern. The AFD is difficult, if not impossible, to remove without physical damage; therefore, criminals prefer an in-situ attack that involves no removal of components. The scope of security then makes certain presumptions that limit risk:

- The POS device stays within the merchant’s environment
- The AFD is virtually impossible to remove and modify (in other words, it would have to be modified in the same location)
- Some degree of surveillance usually augments human presence

Observation Corridors:

- Alteration of the device “in situ”
- “Shoulder surfing” from other customers in the queue
- Distant observation by someone equipped with telescopic optics
- Malicious observation by security cameras
- Hidden cameras in signage and brochure holders

Site Security

Since AFDs are often used without operator presence, video surveillance is recommended. However, orientation of the camera should be managed in a way to prevent observation of the AFD keypad yet allowing the interception of attempts to tamper with the AFD. Means should be considered to allow the customer to block surreptitious observation of the PIN by other people near the AFD. It has been noted that in collusive attacks, the PIN has been captured by someone with binoculars and an accomplice who asks the clerk for a duplicate receipt -- this amplifies the need for the customer to block observation when entering their PIN.

Installation Process

The PIN processing element is a component of the fuelling pump. Safety is the primary consideration when building a fuel pump and POS security is a secondary concern. It is essential that the AFD be installed with robust or non-reversible screws, straps or other mechanisms which would retard installation of a parasite or skimming device.

Inspection Process

The operator should routinely inspect the AFD for signs of tampering including the placement of accessories such as brochure holders and signage. The card reader mechanism should be inspected for evidence of removal and replacement or presence of a "secondary" (or illegal) reader.

Damage to screws and bolts should arouse suspicion and instigate further, more detailed, inspection.

CHAPTER 6

POS PIN & ENCRYPTION SECURITY

Purpose of Recommendations

These PIN security and data encryption recommendations are aimed at providing educational guidelines for the POS Terminals Industry to ensure PIN security and encryption key security are kept at the highest levels possible at all times. In particular, the recommendations are intended for use by all acquiring institutions and agents responsible for PIN transaction processing on the payment card industry participants' denominated accounts. The recommendations should be used in conjunction with applicable industry standards.

Objectives of PIN Security & Key Management

The principle behind POS data encryption and key management is to protect the payment card data and customer entered PIN against unauthorized disclosure, compromise, and misuse throughout the life of a transaction.

This goal can be broken down into the 7 separate objectives listed below, and the requirements and best practices described in this document are aimed at meeting these objectives.

- OBJECTIVE 1** ► Data encryption is used to secure and render data unreadable prior to payment card transaction authorization.
- OBJECTIVE 2** ► Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.
- OBJECTIVE 3** ► Data encryption keys are conveyed or transmitted in a secure manner.
- OBJECTIVE 4** ► Data encryption keys are generated and stored within the POS application; those keys are handled and loaded into hosts and PIN entry devices in a secure manner.
- OBJECTIVE 5** ► Keys are used in a manner that prevents and detects their unauthorized usage.
- OBJECTIVE 6** ► Keys are administered in a secure manner such that documented processes are followed to revoke existing data encryption keys, re-generate new data encryption keys, and re-encrypt existing cardholder data using the new data encryption keys.
- OBJECTIVE 7** ► Procedures used to process data encryption keys, PINs, and keys are managed in a secure manner.

The Scope of PIN & Encryption Security Recommendations

This Chapter contains a complete set of recommendations⁴ for securing PIN data during online and offline payment card transaction processing at POS terminals.

The recommendations are intended for use by all acquiring institutions and agents responsible for PIN transaction processing on the payment card industry participants' denominated accounts and should be used in conjunction with applicable industry standards.

⁴ In order to create a secure environment, networks and acquirers should treat these recommendations as "requirements".

In order to establish a secure environment for PIN based transactions, this Chapter sets out the minimum acceptable 'recommendations'⁵ for securing PINs and encryption keys. Its purpose is to aid all electronic payment system participants in providing the fundamental assurance that cardholder PINs will not be compromised. All participants should incorporate these recommendations in their written procedures.

It should be understood that these recommendations are supplementary to the security requirements defined by the networks. Network requirements should always take precedence over these guidelines.

Security considerations not directly related to PIN processing of transactions are beyond the scope of these minimum PIN and key management security recommendations.

PIN Security Recommendations

General Standards

- a) Data encryption keys and data encryption security procedures should be compliant with the ANSI X9.8 Standard and ISO 9564-1.
- b) The cardholder-entered PIN should be processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs).
- c) The PINs and PIN blocks should not appear in plain text at any point within the network other than in a secure Tamper-Evident Secure Module (TESM) or TRSM or a PIN mailer.
- d) The PIN length should be a minimum of 4 digits and a maximum of 12 digits.
- e) The plain text PIN should never be logged. PIN blocks, even encrypted, should not be retained in transaction journals or logs, except temporarily for audit and fault resolution purposes. Encrypted PIN blocks are required in messages sent for authorization, and must not be retained for any subsequent verification of the transaction.
- f) PINs should be encrypted using a PIN block format that does not produce the same encrypted PIN block for the same PIN for a different card number. [Note that the ISO 9564-1 standard allows format 2 but ANS X9.8 does not.]
- g) All POS connections and host connections to the network should be configured to use line encryption, to provide end-to-end encryption of data.
- h) Acquirers, the network, and issuers should support the ANSI X9.8/ISO 9564 Format 3 PIN block so that an acquirer can ensure response messages are generated by the correct issuer system.

⁵ See footnote 1 above.

Recommendations for PIN, PIN Blocks, & Data Encryption Key at Acquiring Device⁶

- a) The PIN or PIN blocks (PIB) or data encryption keys should not be echoed to the device screen.
- b) The PIN should be encrypted at the keypad or in a TESM directly connected to the keypad such that the PIN and key data cannot be intercepted between the keypad and the TESM. It should not be possible to insert a device between the keypad and the encryption device. Nor should it be possible to recover a data encryption key from a temporary application variable that may use those data encryption keys for securing payment card data.
- c) The PIN, PIN block, and data encryption key should not be in the clear to the application in the device.
- d) The PIN entry device should be configured with full tamper resistance according to industry decreed timings and standards.

Recommendations for the Acquirer Host

- a) The acquirer should only decrypt/encrypt PIN blocks within TRSMs.
- b) The acquirer should maintain adequate key management procedures and processes. These should comply with all parts of ISO 11568.
- c) The acquirer should maintain discrete zones, across which PIN keys will apply.
- d) Unique cryptographic keys should be in use for each identifiable link between host computer systems.

Recommendations for Switches and the Issuer or Authorizing Host

- a) The switch (a computer or electromechanical device that controls routing and operation of a signal path) should only decrypt/encrypt PIN blocks within TRSMs. The switch should maintain adequate key management procedures and processes. These should comply with ISO 11568. The switch should maintain discrete zones, across which PIN keys will apply.
- b) Unique cryptographic keys should be in use for each identifiable link between host computer systems.
- c) Data encryption keys should be protected using key encryption keys within the payment application or POS applications.

⁶ The responsibility for implementing these recommendations should be clearly understood and allocated by the POS deployer or owner.

Recommendations for the Issuer or Authorizing Host

- a) The issuer or authorizing host should validate the PIN by comparing it with stored encrypted values or offsets. The issuer or authorizing host should not store the PIN in the clear.
- b) The issuer or authorizing host should only decrypt/encrypt PIN blocks and compare clear PIN blocks within TRSMs.
- c) The issuer or authorizing host should limit the successive attempted validations by a cardholder with the incorrect PIN. Indication that the PIN is invalid should be included in the response from the issuer or authorizing to the acquirer.

Recommendations for TRSMs

- a) A TRSM should meet the requirements of a physically secure device as defined in ISO 9564-1. Such a device must have a negligible probability of being successfully penetrated to disclose all or part of any cryptographic key or PIN. A TRSM can be certified only after it has been determined that the device's internal operation cannot be modified to allow penetration (for example, the insertion within the device of an active or passive "tapping" mechanism), making it tamper resistant.

A TRSM (for example, a PIN Entry Device (PED)) that complies with this definition may use a Fixed Key or a Master Key/Session management technique, that is, a unique (at least) double-length PIN encryption key for each PED, or may use double-length key DUKPT as specified in ANSI X9.24.2002.

- b) A TRSM relying upon compromise prevention controls requires that penetration of the device, when operated in any manner and in any environment, should cause the automatic and immediate erasure of all PINs, cryptographic keys, other secret values, and any useful residuals of those contained within the device. These devices should employ physical barriers so that there is a negligible probability of tampering that could successfully disclose such a key.

Recommendations for PEDs

- a) PEDs should use encrypting PIN pads that encrypt the PIN directly at the point of entry to meet the requirements for compromise prevention. PEDs that allow cleartext (unenciphered) PINs to travel over cable or similar media from the point of entry to the cryptographic hardware encryption device do not meet this requirement.
- b) Devices that do not retain any key that has been used to encrypt or decrypt secret data, including other keys (for example, DUKPT), require only compromise detection and may be less tamper resistant.

Recommendations for PIN Entry at the Acquiring Device

- a) PIN pads should be located so that they are protected from unauthorized observation.
- b) PIN entry devices should move to encrypting keypads as soon as possible or as part of upgrading to Triple DES.

Recommendations for PIN Pad Security

- a) Prior to connection to a POS network, a POS should be certified to have a tamper-resistant PIN pad that meets the stated requirements of the network. Networks may elect to accept certification announcing that the PIN pad meets the requirements set by other networks (such as Visa/MasterCard) if those requirements meet or exceed those of the network.
- b) Members who wish to deploy a new device type should begin by inquiring with the vendor or against official lists of Certified Devices to determine if the device type has already been certified. If the device type is included on the List of Certified Devices, the member should obtain a copy of the device certificate from one of the device vendors or from the device certification agent prior to connecting the device.
- c) For device types not included on relevant lists of Certified Devices, a member or the device vendor should contact a device certification agent to arrange for testing and certification of the device type.
- d) If the manufacturer has had the device certified, it can be sold as a certified device that will incur no further certification costs prior to installation.
- e) A manufacturing change to a device means that the device should be re-certified.
- f) When any modification is made to any component or attribute of the device that is subject to certification, the device should be re-certified prior to deployment; re-certification is required for all modifications to a device unless none of the modifications affect a component or attribute that is subject to certification.
- g) Deployers should keep a current published list of all its certified POS devices in operation.
- h) Networks should set dates for compliance of new devices, replacement devices, and existing devices. The dates set for each category of device should be appropriate to the potential risk of compromise at non-compliant devices. Devices identified as non-compliant will either not be permitted to be connected to the network, or, in the case that installed PIN pads, a request should be filed for exemption status. Otherwise, removal of the POS will be required. **Note:** Deployed devices must meet the requirements of all networks for which the devices acquires transactions.

Recommendations for PIN Translation & Encryption

- a) All cardholder PINs processed online should be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards.
- b) Online PIN translation should only occur using one of the allowed key management methods: DUKPT, Fixed Key, or Master Key/Session Key.
- c) Online PINs should be encrypted using the TDEA Electronic Code Book (TECB) mode of operation as described in ANSI X9.52. For purposes of these recommendations, all references to ECB are using key options 1 or 2, as defined in ANSI X9.52. Schemes may allow alternative methods if validated as at least as secure as TDES.
- d) All cardholder PINs processed offline using Integrated Circuit (IC) card technology should be protected in accordance with the requirements in Book 2 of the EMV2000 IC Card Specifications for Payment Systems.⁷
- e) For online transactions, PINs should only be encrypted using ISO 9564–1 PIN block formats 0, 1, or 3. Format 2 should be used for PINs that are submitted from the IC reader to the IC.
- f) For secure transmission of the PIN from the point of PIN entry to the card issuer, the encrypted PIN block format should comply with ISO 9564–1 format 0, ISO 9564-1 format 0,1, or 3. Schemes may allow for alternative methods on a case-by-case basis.
- g) For ISO format 0 and 3, the cleartext PIN block and the primary account number block should be XORed together and then Triple DES encrypted in Electronic Code Book (ECB) mode to form the 64-bit output cipherblock (the reversibly encrypted PIN block). Note that as stated in recommendation (f) above, a scheme approved alternative encryption method may be used.
- h) ISO format 3 should be used for encryption zones where the PIN encryption key is static for the productive life of the device in which it resides.
- i) PINs enciphered only for transmission between the PIN entry device and the IC reader should use ISO format 0, 1, or 3. Formats 0,1 and 2 are less secure than format 3 since they do not bind the account number to the PIN. ISO Format 2 may only be used if encrypted with a unique key per transmission.

⁷See sections 7 and 11.1.2 of Book 2 of the EMV2000 IC Card Specifications for Payment Systems.

- j) PINs should not be stored **except** as part of a store-and-forward transaction as noted in ISO 9564-1 and then only for the minimum time necessary. Any store-and-forward transaction PIN should be stored in encrypted form using a unique key not used for any other purpose. **Note:** Store-and-forward is a practice not compliant with PCI requirements. Compensating controls must be in place if this is necessary.
- k) Host Security Module (HSM) Master File Keys, including those generated internal to the HSM and never exported, should be at least double-length keys and use the TDEA.

Key Management Recommendations

In order to protect the secrecy of a PIN that has been encrypted using DES or Triple DES, it is vital that the key used for encrypting and decrypting is also kept secret. It is particularly important that great care be exercised in order to protect the cleartext components of a key as they pass through the various lifecycles.

The practices and recommendations defined in this chapter, while not necessarily exhaustive, are considered effective in protecting the secrecy of encryption keys and their components⁸.

General Recommendations

Usage

- a) Keys should be unique:
 - i. All keys used in a PED, whether for key encryption or PIN encryption, should be unique to that device.
 - ii. Terminal Master Keys (TMKs) and any keys used to load TMKs should be unique to the device being loaded.
 - iii. In a master/session key approach, the master key(s) and all session keys should be unique to each cryptographic device.
 - iv. Where a PED interfaces with more than one acquirer, the PED TRSM should have a completely different and unique key(s) for each acquirer. These should be totally independent and not variants of one another.
 - v. Keys that are generated by a derivation process and derived from the same base key should use unique data for the derivation process. This ensures that all cryptographic devices receive unique initial keys.

⁸ For more guidance on key management the reader is referred to the White Paper produced by K3DES LLC, Effective Encryption Key Management Practices, available at ATMIA's Best Practice Online Resource Center at <http://www.atmianortham.com/ResourceCenter/atmresourcecenter.asp> and on the GASA website at www.globalasa.com.

- vi. Zone encryption should be used for communication between organizations, and unique keys should be used for each identified link between host computer systems.
- b) PIN encryption keys should be held in only the PED and in security modules at the minimum number of locations consistent with effective operation. Disclosure of the key in one device should not provide information that could feasibly be used to determine the key in any other such device.
- c) Keys may exist at more than one pair of locations for load balancing purposes, for example in dual processing sites.
- d) Encryption keys should only be used for the purpose they were intended, so as to minimize exposure should a key be compromised. For example, a Key Encryption Key should never be used as a PIN Encryption Key.
- e) Keys should never be shared or substituted on a processor's production and test system.
- f) No key or key component should ever exist outside a TRSM except when encrypted or securely stored and managed using the principles of dual control and split knowledge.

Dual Control & Split Knowledge

As in DES and Triple DES, the same key is used to encrypt and decrypt. **The principles of dual control and split knowledge are fundamental to the protection of encryption keys. These principles should be applied throughout all key lifecycle stages and included in relevant written procedures.**

- a) Dual control means that at least two authorized individuals are required to work in partnership to carry out an activity, such as generating, storing, or loading the cleartext components of a key.
- b) Split knowledge means that no single individual knows, or has access to, a whole entity, be it all the cleartext components of a key, or the combination of a safe where key components are stored.

In order to implement these principles, an organization should designate certain individuals as key custodians. Each key custodian should be assigned responsibility for specific key components throughout their lifecycle. They may be responsible for more than one key component as long as no two components form part of the same key, because this would compromise the principle of split knowledge.

One key custodian may be a back-up to another key custodian but only where the principle of split knowledge would not be compromised. A key custodian should not back up another key custodian if this will cause them both to be responsible for components belonging to the same key.

In order to reduce the opportunity for key compromise, the number of key custodians should be limited to the minimum number required. In general the designation of a primary and a back-up key custodian for each component should be sufficient. This designation should be documented by having each custodian sign a key custodian form. The form should specifically authorize the custodian and identify the custodian's responsibilities for safeguarding key components or other keying material entrusted to them.

The key custodians should have no connection or reporting relationship to other key custodians.

Witnessing Key-Related Events

Even with the principles of dual control and split knowledge in place, it is recommended that certain lifecycle events be witnessed and signed off by a third-party.

This third-party should have no relationship with the key custodians involved. At a minimum key-related events that should be witnessed are:

- a) Generation of encryption keys
- b) Erasure of encryption keys
- c) Destruction of cleartext encryption key components, regardless of the media they are on

The witness should be given a copy of the script or procedure in use so that they can follow the process. The witness should sign an affidavit that states that the activity was carried out completely and correctly. Any deviations from the script or procedure should be noted and explained. The affidavits form part of the auditable records of the key management process and should be kept indefinitely.

Documentation, Administration & Logging

For the effective management of encryption keys and their components, certain procedures, logs, and forms should be in place.

- a) Documented procedures should exist and be in use for:
 - i. All key generation processes
 - ii. All key transmission and conveyance processes
 - iii. All key loading activities
 - iv. All key compromise activities, including replacement of compromised keys, escalation processes, damage assessment, and remediation
 - v. All key destruction activities

- b) An encryption key log should be maintained for all actions related to key components. At a minimum, this log should contain:
- i. The name and signature of the authorized key custodian
 - ii. The type of key
 - iii. The number of the component
 - iv. The date and time of the action
 - v. The serial number of the tamper-evident envelope
 - vi. The action undertaken

The log should be periodically audited by an independent group, such as Information Security, for completeness and accuracy. The encryption key log should be kept in a tamper-evident envelope in a secure place like a safe. Its removal from the safe and its tamper-evident envelope should be recorded.

- c) In addition to the log mentioned above, certain other forms should be used to record activities undertaken with regard to keys and key components. At a minimum, these forms should include:
- i. A form to record encryption key component values and corresponding check sum values
 - ii. A form for recording encryption key components being transported
 - iii. A log for recording key loading activities
 - iv. A form for recording PINs used to access smart cards that contain key components
 - v. A form for recording any passwords needed to activate any equipment used
 - vi. Affidavits for the generation or destruction of keys and key components

These forms along with the encryption key log form the basis for auditing key management processes. They should be complete and contain as much information as possible. They should be securely stored and made available to those individuals conducting an audit.

Back-Ups

In principle, unique keys, once loaded, should not be retained even for the purposes of back-up. Please note that it is not a requirement to have back-up copies of key components or keys. However, for other keys:

- a) Back-ups of secret keys should exist only for the purpose of reinstating keys that are accidentally destroyed. The back-ups should exist only in one of the allowed storage forms for that key.

- b) Creation and management of back-up copies should be under dual control, they should be securely stored with proper access controls, and they should be subject to at least the same level of security as keys in use.
- c) Back-ups (including cloning) should require a minimum of two authorized individuals to enable the process.

Specific Recommendations for Key Encryption

- a) All DES keys used for encrypting keys for transmittal should be at least double-length keys and use the TDEA in an encrypt or decrypt mode of operation for key encipherment.
- b) A double- or triple-length DES key should not be encrypted with a DES key of a shorter length.
- c) RSA keys used to transmit or convey other keys should use a key modulus of at least 1024 bits.⁹
- d) DES keys that are used to encrypt other keys or to encrypt PINs and that exist outside of a TRSM should be encrypted using either TDEA (using at least double-length keys) or RSA (using a key modulus of at least 1024 bits). Schemes may allow alternative methods if validated to be at least as secure as Triple DES.
- e) Symmetric secret keys may be encrypted using public key cryptography for distribution to PEDs as part of a key-establishment protocol.
- f) Key variants should only be used in devices that possess the original key.
- g) Although a key used to protect the PIN Encrypting Key should never be used for any other cryptographic purpose. Variants of the same key may be used for different purposes.
- h) Variants of a Master File Key should not be used external to the (logical) configuration that houses the MFK itself.

Specific Recommendations for Key Generation

The following is a list of the specific recommendations related to key generation. Please bear in mind that these are in addition to those recommendations already given in Key Management Recommendations section of this chapter, particularly those related to dual control and split knowledge and documentation and logging.

⁹ As of June 2004. Key lengths should be periodically re-evaluated.

- a) All keys and key components should be generated using a random or pseudo-random process that is capable of satisfying the statistical tests of FIPS 140-2 level 3.
- b) Keys should be generated so that it is not feasible to determine that certain keys are more probable than other keys from the set of all possible keys.
- c) An independent assessor should certify self-developed implementations of a cryptographic pseudo-random number generator.
- d) The output of the key generation process should be monitored to ensure there is no unauthorized tap or other mechanism that might disclose a cleartext key or key component as it is transferred between the key generation TRSM and the device or medium receiving the key or key component.
- e) Printed key components should be printed within blind mailers or sealed immediately after printing so that only the entrusted party can observe each component. This helps detect tampering.
- f) Any residue from the printing or recording process that might disclose a component should be destroyed before an unauthorized person can obtain it.

Specific Recommendations for the Transfer, Conveyance, and Distribution of Cleartext Components

The following is a list of the specific recommendations related to the transfer, conveyance and distribution of cleartext key components. Please bear in mind that these are in addition to those recommendations already given, particularly those related to dual control and split knowledge, and documentation and logging.

- a) When a private or secret key is being physically forwarded, it should be sent as a minimum of two separate components:
 - i. Each component should be transferred in a tamper-evident package or within a TRSM.
 - ii. Each component should be sent via different communication channels like different courier services. It is not sufficient to send the key components for a specific key by the same courier on different days.
- b) Private and secret keys may also be transferred by transmitting the key in ciphertext form provided that this does not compromise the principle of split knowledge or the level of security in general.
- c) All key encryption keys used to transmit or convey other cryptographic keys should be (at least) as strong as any key transmitted or conveyed.

- d) Public keys should be conveyed in a manner that protects their integrity and authenticity and should use a mechanism independent of the actual conveyance to provide the ability to validate receipt of the correct key.
- e) No person should have access to any cleartext key component during the transport process.
- f) Mechanisms should exist to ensure that only authorized custodians place key components into tamper-evident packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components.
- g) Any single unencrypted key component should be at all times during its transfer, conveyance, or movement between any two organizational entities:
 - i. Under the continuous supervision of a person with authorized access to this component,
 - or,
 - ii. Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it,
 - or,
 - iii. In a physically secure TRSM managed under the strict principles of dual control and split knowledge.
- h) Key establishment protocols using public key cryptography may also be used to distribute PED symmetric keys. These key establishment protocols may use either key transport or key agreement. In a key transport protocol, the key is created by one entity and securely transmitted to the receiving entity. For a key agreement protocol, both entities contribute information, which is then used by the parties to derive a shared secret key.
- i) A public key technique for the distribution of symmetric secret keys should:
 - i. Use public and private key lengths that are deemed acceptable for the algorithm in question (for example, 1024-bits minimum for RSA);
 - ii. Use key-generation techniques that meet the current ANSI and ISO standards for the algorithm in question;
 - iii. Provide for mutual device authentication for both the host and the PED. This includes assurance to the host that the PED actually has computed the session key or actually can compute the session key and that no other entity other than the PED specifically identified can possibly compute the session key.

Specific Recommendations for Key Component Storage and Physical Access

Please note that this section refers to keys and key components prior to their being loaded. Unique keys and their component parts should not be kept once they have been loaded. These recommendations are in addition to those given in this chapter regarding dual control and split knowledge and documentation and logging.

- a) Printed or magnetically recorded key components should reside only within tamper-evident sealed envelopes so that the component cannot be ascertained without opening the envelope.
- b) The media upon which a component resides should always be physically safeguarded.
- c) Components for a specific key that are stored in separate envelopes but within the same secure container, place reliance upon procedural controls and do not meet the requirement for physical barriers.
- d) Furniture-based locks or containers with a limited set of unique keys are not sufficient to meet the requirement for physical barriers.
- e) No one but the authorized key custodian (and designated back-up) should have physical access to a key component.
- f) Key components may be stored on tokens (for example, PC cards, smart cards, and so forth). These tokens should be stored in such a manner as to prevent unauthorized individuals from accessing the key components. For example, if key components are stored on tokens that are secured in safes, more than one person might have access to these tokens. Therefore, additional protection is needed for each token (possibly by using tamper-evident envelopes) to enable the token's owner to determine if a token was used by another person. Key components for each specific custodian should be stored in separate secure containers.
- g) If a key is stored on a token and a PIN or similar mechanism is used to access the token, only that token's owner (or designated back-up) should have possession of both the token and its corresponding PIN.

Specific Recommendations for Key Loading and Entry

The following is a list of the specific recommendations related to the key loading and entry. Please bear in mind that these are in addition to those recommendations already given, particularly those related to dual control and split knowledge, and documentation and logging.

- a) All keys when loaded from individual cleartext components should be loaded using the principles of dual control and split knowledge.

- b) Manual key loading may involve the use of media such as paper or specially designed key-loading hardware devices. For devices that do not support the entry of full-length components, two or more components should be created and used.
- c) Any TRSM loaded with the same key components should combine all entered key components using the identical process.
- d) Any mechanisms used to load keys, such as terminals, external PIN pads, or key guns, should be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.
- e) Prior to key loading, TRSM equipment should be inspected to detect any evidence of monitoring or tampering.
- f) Plaintext keys and key components should be transferred into a TRSM only when it can be ensured that there is no tap at the interface between the conveyance medium and the cryptographic device that might disclose the transferred keys. It should also be ensured that the device has not been subject to any prior tampering which could lead to the disclosure of keys or sensitive data.
- g) A TRSM should transfer a plaintext key only when at least two authorized individuals are identified by the device (for example, by means of passwords or other unique means of identification).
- h) The injection of key components from an electronic medium to a cryptographic device (and verification of the correct receipt of the component is confirmed, if applicable) should result in either of the following: the medium is placed into secure storage, if there is a possibility it will be required for future re-insertion of the component into the cryptographic device, or all traces of the component are erased or otherwise destroyed from the electronic medium.
- i) For keys transferred from the cryptographic hardware that generated the key to an electronic key-loading device:
 - i. The key-loading device should be a physically secure TRSM that is designed and implemented in such a way that any unauthorized disclosure of the key is prevented or detected;
 - ii. The key-loading device should be under the supervision of a person authorized by management or should be stored in a secure container so that no unauthorized person can have access to it;
 - iii. The key-loading device should be designed or controlled so that only authorized personnel under dual control can use and enable it to output a key into another TRSM. Such personnel should ensure that a key-recording device is not inserted between the TRSMs;

- iv. The key-loading device should not retain any information that might disclose the key or a key that it has successfully transferred.
- j) Any tokens, Erasable Programmable Read-Only Memory devices (EPROMs), or other key component holders used in loading encryption keys should be maintained using the same controls used in maintaining the security of hard copy key components. These devices should be in the physical possession of only the designated component holder and only for the minimum practical time.
- k) If the component is not in human comprehensible form (for example, in a programmable read-only module (PROM), in a smart card, on a magnetic stripe card, and so forth), it should be in the physical possession of only one entity for the minimum practical time until the component is entered into a TRSM.
- l) If the component is in human readable form (for example, printed within a PIN mailer type document), it should only be visible at one point in time to only one person (the designated key custodian) and only for the duration of time required for this person to privately enter the key component into a TRSM.
- m) Printed key component documents should not be opened until just prior to entry.
- n) All hardware and passwords used for key loading should be managed under dual control.
- o) Any hardware used in the key-loading function should be controlled and maintained in a secure environment under dual control. Use of the equipment should be monitored and a log of all key-loading activities maintained for audit purposes. All cable attachments should be examined before each application to ensure they have not been tampered with or compromised.
- p) Any physical key(s) (for example, brass keys) used to enable key loading should not be in the control or possession of any one individual who could use those keys to load cryptographic keys under single control.
- q) The loading of keys or key components should incorporate a validation mechanism so that the authenticity of the keys is ensured. It should also be possible to ascertain that the keys or key components have not been tampered with, substituted, or compromised.

Specific Recommendations for Key Compromise and Destruction

The following is a list of the specific recommendations related to key compromise and destruction. Please bear in mind that these are in addition to those recommendations already given, particularly those related to dual control and split knowledge and documentation and logging.

- a) The compromise of a key requires the destruction of that key, all variants and non-reversible transformations of that key, and all keys encrypted under or derived from that key. Likewise, known or suspected substitutions of a secret key requires destruction and replacement of that key and any associated key encipherment keys.
- b) A cryptographic key should be replaced with a new key whenever the compromise of the original key is known or suspected. In addition, all keys encrypted under or derived using that key should be replaced with a new key within the minimum feasible time. The replacement key should not be a variant of the original key or an irreversible transformation of the original key.
- c) Key components should never be reloaded when there is any suspicion that either the originally loaded key or the device has been compromised. If suspicious alteration is detected, new keys should not be installed until the TRSM has been inspected and assurance reached that the equipment has not been subject to unauthorized physical or functional modification.
- d) Specific events should be identified that would indicate a compromise may have occurred. Such events may include, but are not limited to:
 - Missing cryptographic devices
 - Tamper-evident seals or envelope numbers or dates and times not agreeing with log entries
 - Tamper-evident seals or envelopes that have been opened without authorization or show signs of attempts to open or penetrate
 - Indications of physical or logical access attempts to the processing system by unauthorized individuals or entities

Procedures should require that plaintext key components stored in tamper-evident envelopes that show signs of tampering should result in the destruction and replacement of the set of components, as well as any keys encrypted under this key.

- e) If attempts to load a key or key component into a cryptographic device fail, the same key or component should not be loaded into a replacement device unless it can be ensured that all residue of the key or component has been erased or otherwise destroyed in the original device. Instances of keys or key components that are no longer used or that have been replaced by a new key should be securely destroyed.

Keys maintained on paper should be burned, pulped, or shredded in a cross-cut shredder. If the key is stored in Electronically-Erasable Programmable Read-Only Memory devices (EEPROMs), the key should be overwritten with binary 0s (zeros) a minimum of three times. If the key is stored on EPROM or PROM, the chip should be physically destroyed in such a way as to leave it unusable and un-repairable. When possible it should be broken into pieces and the pieces disposed of separately.

Other permissible forms of a key instance (physically secured, enciphered or components) should be destroyed following the procedures outlined in ISO-9564-1 or ISO-11568-3. In all cases, a third party (other than the custodian) should observe the destruction and sign an affidavit of destruction.

- f) Key encipherment key components used for the conveyance of working keys should be destroyed after successful loading and validation of the working key.
- g) Documented procedures should exist, be known by all affected parties, and be demonstrably in use for:
 - i. Replacement of compromised keys, including subsidiary keys (for example, those keys enciphered using the compromised key) to a value not feasibly related to the original key;
 - ii. An escalation process including notification to organizations that currently share or have previously shared a suspect key. The procedures should also include damage assessment and details of specific actions to be taken with system software and hardware, keys, encrypted data, and so forth.
- h) Controls and procedures should also exist to prevent or detect the unauthorized substitution of one key for another; thereby, reducing the risk of an adversary substituting a key known only to them. These procedures should include investigating multiple synchronization errors.
- i) To prevent substitution of a compromised key for a legitimate key, key component documents that show signs of tampering should result in the discarding and invalidation of the component and the associated key at all locations where they exist.

Specific Recommendations for Key Equipment Management

The following is a list of the specific recommendations related to the management of key equipment. Please bear in mind that these are in addition to those recommendations already given, particularly those related to dual control and split knowledge, and documentation and logging.

- a) Hardware Security Modules (HSMs) and PEDs should only be placed into service if there is assurance that the equipment has not been subject to unauthorized modification, substitution, or tampering. This requires physical protection of the device up to the point of key insertion or inspection, and possibly testing of the device immediately prior to key insertion. Techniques include the following:
- Cryptographic devices are transported from the manufacturer's facility to the place of key-insertion using a trusted courier service. The devices are then securely stored at this location until key-insertion occurs.
 - Cryptographic devices are shipped from the manufacturer's facility to the place of key-insertion in serialized, counterfeit-resistant, tamper-evident packaging. Devices are then stored in such packaging or secure storage until key-insertion occurs.
 - The manufacturer's facility loads into each cryptographic device a secret, device-unique "transport-protection token." The TRSM used for key-insertion has the capability to verify the presence of the correct "transport-protection token" before overwriting this value with the initial key that will be used.
 - Each cryptographic device is carefully inspected and tested immediately prior to key-insertion using due diligence. This is done to provide reasonable assurance that it is the legitimate device and that it has not been subject to any unauthorized modifications.
- b) Records should be maintained of the tests and inspections given to PIN-processing devices before they are placed into service, as well as devices being decommissioned.
- c) Controls should exist to ensure that a counterfeit device possessing all the correct operational characteristics plus fraudulent capabilities has not been substituted for a legitimate device.
- d) Notwithstanding how the device is inspected and tested, the device serial number should be verified against the purchase order, invoice, waybill, or similar document to ensure that device substitution has not occurred.
- e) Devices should incorporate self-tests to ensure their correct operation. Devices should not be re-installed unless there is assurance they have not been tampered with or compromised.
- f) Key and data storage should be zeroized when a device is decommissioned.
- g) If necessary to comply with the above, the device should be physically destroyed so that it cannot be placed into service again or cannot allow the disclosure of any secret data or keys.

- h) Any TRSM capable of encrypting a key, and producing cryptograms of that key, should be protected against unauthorized use. This protection takes the form of either or both of the following:
 - i. Dual access controls are required to enable the key encryption function
 - ii. Physical protection of the equipment with access under dual control
- i) Cryptographic equipment should be managed in a secure manner in order to minimize the opportunity for key compromise or key substitution. That is to say, physical keys, authorization codes, passwords, or other enablers should be managed under dual control and split knowledge.
- j) Controls should exist and be in use to ensure that all physical and logical controls and anti-tamper mechanisms are not modified or removed.
- k) Documented procedures should exist, be known by all affected parties, and be demonstrably in use for the following:
 - Inventory control and monitoring allowing equipment to be tracked by both physical and logical identifiers, so as to protect equipment against unauthorized substitution or modification or to detect lost or stolen equipment
 - Destruction of all keys and PINs or related data within a cryptographic device when that device is removed from service
 - The security and integrity of PIN processing equipment as it is placed into service, initialized, deployed, used, and decommissioned (these should include the principles for dual control and split knowledge)
 - Physical security and access to host TRSMs

Key Management Procedures

Recommendations for Key Management Procedures

Only key management procedures agreed by the network can be used. Members may submit proposals for other procedures to the network for agreement.

- a) Zone Master Keys (ZMKs), Zone PIN Keys (ZPKs), Terminal Master Keys (TMKs), and Terminal PIN Keys (TPKs) should be changed at a frequency appropriate for the risk or believed compromised.
- b) No individual should have access to the complete, plaintext ZMK, ZPK, TMK, TPK, or more than one of its components, and there should be controls to prevent and detect possible compromises.

- c) The ZMK, ZPK, TMK, or TPK should be generated using a process that makes it impossible to predict any character in the key from any of its components. The components will typically be combined using an XOR process and not a sequence of the components.
- d) There should be a unique TMK for each PIN pad. Intentional use of duplicate TMKs is not allowed.
- e) TPKs should be distributed and stored securely.
- f) The person who generates a Key Encrypting Key (KEK), (for example, the ZMK or TMK) should not be allowed to generate the PIN key encrypted under that KEK, (for example, ZPK or TPK) unless it is part of an automated process.
- g) All Zone and PIN keys should be unidirectional. The same key should not be used for both the acquirer zone and issuer zone.
- h) Three components should be used in the generation of a ZMK.
- i) Key components for manual loading should only be delivered in tamper-evident envelopes.

Guidelines for Key Management Procedures

- a) Single-length ZMKs, if permitted, should be changed at least once every 6 months.
- b) Single- & double-length ZPKs and TPKs should be changed at least daily.
- c) Double-length ZMKs should be changed at least every twelve months.
- d) The network and the members should investigate the advantage of moving to a Public Key Infrastructure (PKI) or other suitable method for distributing ZMKs and TMKs.
- e) Keys and key components should be generated with check values and the check values should be verified when loaded remotely.

Cryptography Best Practice Recommendations

Objective

The cryptographic algorithms and key lengths shall be such that the likelihood of finding the key or the data it is protecting is low during the life of the key.

The objective of key management is to provide the users with the keys that they need to perform the required cryptographic operations and to control the use of those keys. It ensures that the keys are protected during their lifecycle. This protection minimizes the opportunity for a security breach and its consequences. It maximizes the probability of detection of any illicit access or change to key.

Recommendations for Algorithms

- a) Only algorithms approved by the network for PIN block encryption should be used. Currently only the DES algorithm is permitted.
- b) The connection between the member host and the network should use Triple DES, as defined in ANSI X9.52.
- c) The connection between the POS and acquirer host should use a hardware implementation of Triple DES, as defined in ANSI X9.52 and according to industry decreed timings.

Recommendations for Key Length

- a) Only Key lengths approved by the network should be used.
- b) Double-length (112 bit) DES keys (ZPKs and ZMKs) should be used between each member and the network.
- c) All TMKs and TPKs should be double-length (112 bit) keys or use an approved more secure encryption method according to industry decreed standards.

CHAPTER 7

POS SOFTWARE SECURITY

The Role of POS Software

All point of sale (POS) terminal hardware utilizes software to operate the hardware and to process transactions. Initially all POS payment card transactions were paper based. This process was slow and inefficient, and very risky for the issuer since they could not verify the authenticity of a card or cardholder and dumpster diving for paper receipts became a serious problem. The card payment industry and merchants started moving into electronic transaction processing of card transactions at the point of sale. POS equipment at the time ran on proprietary software and hardware and used dial-up telephone lines to authorize transactions.

Today we are seeing open POS systems with standardized software and Internet connectivity for transaction authorization. All of these changes have made the payment card processing environment more flexible, stable and efficient. These changes also introduce new risks to organizations' computer networks and the software used to process card payment transactions.

This chapter addresses the various aspects of software security in the POS device/computer operating environments.

Processing POS Transactions using TCP/IP Over the Internet

Merchants are always looking for ways to reduce costs and improve their customers' experience. Now that many merchants have a dedicated high speed Internet connection that is utilized for many back office purposes, it makes sense to eliminate the dedicated phone line they use for POS transactions. This saves money on the dedicated phone lines and merchants can also reduce the transaction processing time to a fraction of the time it takes to dial-up for an authorization.

While TCP/IP can be made more secure than a dial-up Public Switched Telephone Service (PSTN), the connectivity to the Internet opens a host of other potential vulnerabilities if the merchants' internal network and systems are not properly secured and maintained.

POS transactions that are processed over the Internet will normally travel through a merchant's internal computer network and use an always-on high speed Internet connection. This connectivity has driven criminals to attempt to hack into merchant networks through the Internet or through wireless access points at the merchant locations.

Networks should be protected with a dedicated firewall between the Internet and internal network to protect sensitive data from unauthorized access. This type of access can originate from un-trusted hosts, external networks and unauthorized persons attaching to a local network.

To mitigate these risks, merchant networks should establish a detailed security policy for the overall network and each device on the network. A configuration policy for the Internet firewall is particularly important. The policy should include changing default settings to support only required ports and services. Any default passwords should be changed to strong passwords using at least 8 alphanumeric and special characters. All vendor security patches and updates should be tested and implemented as quickly as possible.

Ensure that card track data, full card number or PIN is never stored anywhere in the POS software system.

Ensure that you have a point of contact for security issues at each merchant who uses your software and you have a security point person on staff in case of compromises or emergency security patch alerts and delivery mechanisms.

Virtual Terminals

A virtual terminal is a software program designed to run on computers that also tend to be used for other purposes. A configuration policy for computers running virtual terminals is particularly important. The policy should include changing default settings to support only required services. Any default passwords should be changed to strong passwords using at least 8 alphanumeric and special characters. All vendor security patches and updates should be tested and implemented as quickly as possible.

Any custom or modified code that is installed on computers running in a network or used with virtual terminals should be tested for security vulnerabilities prior to implementation. These changes may open new vulnerabilities and vendor security patches and updates will not secure them.

Tracer Programs

A tracer program is used to test and/or troubleshoot a POS software and hardware environment in a merchant location. Tracer programs log all of the transaction data from a terminal or terminals and are very useful for troubleshooting purposes, however, they are a tremendous vulnerability. If the program is left running or installed on a computer that is accessed by a criminal where it can be switched on; all data including sensitive data will be recorded and can be accessed by criminals or rogue employees. A policy on tracer programs should include who has access to use the programs and under what circumstances. Also the policy should include how programs are stored, installed, uninstalled and how any data that has been logged is destroyed.

POS Software Development

All software development should follow a documented systems development lifecycle (SDLC). This process should document and cover: functional requirement specifications, system design, secure coding standards, code review, testing, defect and resolution tracking and configuration management.

Security and reliability are critical elements in POS software design. Many reliability issues will result in security vulnerabilities. Incorporating good security design and testing upfront will ultimately create a better product requiring less support for the lifecycle of the product.

POS software security design should incorporate simple and open security mechanisms. The less proprietary code and complexity in the security procedures means easier maintenance and verification of the level of security that exists in the software. This is very important with the new PCI PABP (Payment Card Industry Program Application Best Practices) requirements that are coming out. All processors and merchants will be responsible for maintaining the security of the data in their environment, and the more open and proven security a software vendor provides is a big selling point.

Concepts used for secure software design include:

- Granting users and procedures the minimum privileges to complete a process
- Using explicit access rights
- Verifying access to objects
- Using layered security mechanisms so when one mechanism is compromised, it will not allow full compromise of the system or communications
- System failing in a secure manner
- System logging any data related to the failure

Antivirus Software

Antivirus software should be used throughout the development cycle and by organizations deploying the software to maintain security. Vendors should consider providing antivirus software to end users of the software. It is important to ensure the antivirus software is updated and run regularly on computers that touch the transaction path, especially virtual terminals.

Cryptography

Documentation should be developed for end users and installers that covers all aspects of the POS software implementation of key management. Include a discussion of the merchant's key management responsibilities and the impact of key compromise. Industry standard secure algorithms should be implemented instead of proprietary or non-standard algorithms. Use secure protocols such as IPSec, SSL/TLS or SSH to encrypt and protect software key management processes which use insecure protocols¹⁰. Also include error handling that will identify and reject key updates that fail an integrity check. Incorporate processes to alert the merchant or processor of these events.

Penetration Attacks

Criminals will attempt to penetrate POS software security by attempting to impersonate a terminal/transaction using information about transactions such as the sequence number, and by modifying other parts of the transaction. Criminals will replay transactions, sending random sequence numbers to impersonate a legitimate terminal. To mitigate these risks, use techniques to make each transaction and each session unique, such as sequence numbers and transaction timestamps. The more information used in this process will make it that much more difficult for an illegitimate transaction to be created. Also include documented error handling that will identify these situations and alert the merchant or processor.

Criminals will use programs, called Trojan horses, surreptitiously installed and running on the terminal computer to log and transmit transaction data. Trojan horse programs can be installed by email viruses, compromised legitimate software or surfing websites that have been compromised to download these programs to web client computers. It is critical that a computer running virtual terminal software is only installed with specific applications that have gone through a security review to ensure they are not carrying a Trojan program. Running software that checks the state of applications at system start-up will minimize the chance of using the system when it has been compromised. Allowing the user to install applications should be restricted to minimize risk.

Client web browsers can be exploited by visiting a compromised website. Any web server on the Internet can be a threat if the web browser is running on a computer with POS software. This type of compromise can disclose information residing on the computer such as cookies and files, allow execution of arbitrary code, or allow the criminal to take control of the computer.

¹⁰ Such as FTP, TFTP or SNMP protocols.

Disabling Active X, Java Virtual Machine, Java, Javascript, file downloads, active scripting, IFRAME and 'enable on demand' in Internet Explorer will limit some of these vulnerabilities. Use of an open source web browser with unnecessary functionality removed is another option and is likely a safer alternative to Microsoft browsers. Regardless of which browser used on a computer, it should be the latest version with the latest security patches kept up-to-date.

Internet Protocols

Internet protocols are used to manage the movement of data and access to computers across local networks and the Internet. Most of the well known protocols have been around for decades and were not securely designed, or the security originally designed in is now obsolete. These protocols were designed for ease of use and, at that time, the Internet was not as open or widely used as it is today.

When designing and implementing POS software systems; always choose the most secure protocols such as IPSec, SSL/TLS or SSH. If an insecure protocol such as FTP, TFTP or SNMP is utilized, then wrap the insecure protocol with a secure protocol to ensure it is protected. Since DNS servers and lists can be compromised, secure protocols should not rely on a DNS server to return the correct IP address upon lookup. All protocol vendor security updates should be tested and applied as soon as possible to reduce compromise risks. Vendor documentation should include all third-party software so updates can be monitored and managed.

The FTP protocol should be avoided; instead, consider using SCP over SSH. If an FTP is used to transfer files, there are several best practices that need to be followed. Install the FTP server as a non-privileged user, isolate it on a separate partition or file system and disable anonymous access. Create specific user accounts with appropriate permissions that tie to appropriate file permissions on FTP directories. Keep FTP server (and client) software up-to-date with vendor security updates.

HTTP servers are attacked using buffer overflow vulnerabilities, execution of poorly coded scripts and inadequate user access control on directories or default installation passwords. There are several best practices that need to be followed for HTTP servers. Install the HTTP server as a non privileged user, isolate it on a separate partition or file system, change the default passwords and ensure passwords are transmitted between HTTP clients via SSL. Change the banner indicating the web server type and software version to avoid automatic detection by criminals. Remove all unneeded functionality including example source code and sample applications. Keep HTTP server (and client) software up to date with vendor security updates.

Telnet is a protocol used to remotely log into other computers connected on a network. Telnet is insecure since the username, password and data are not encrypted. Do not use telnet, use Secure Shell (SSH).

SSH provides an encrypted terminal session to log onto other computers connected on a network. Other insecure protocols can be wrapped in SSH to protect them. SSH version 2 is more secure and recommended over SSH version 1. When implementing SSH version 2, use AES or 3DES and avoid using rhosts, which rely on IP addresses for authentication. Implement self tests and a strong random number generator to reduce risk. Use a documented and strong key management process since breakdowns in this process can lead to compromise of the encryption keys.

Secure Socket Layer (SSL) is used to create secure and reliable end-to-end security. The SSL Handshake Protocol is used to authenticate and negotiate the algorithms and keys between the two computers attempting to communicate. The SSL Change Cipher Spec Control is used to manage and updating the computer connection. The SSL Alert Protocol is used to send SSL related alert information. The Transport Layer Security (TLS) protocol is a standardized version of SSL version 3. The TLS version 1 protocol is more secure and recommended over SSL. When implementing TLS version 1, use 3DES with a 128 bit key length for encryption, use SHA-1-512 for data integrity and DHE, and DH or RSA for key establishment. Never use anonymous Diffie-Hellman key exchange since it is less secure and susceptible to attacks. Use Public Key cryptography based on RSA or DSA for server authentication and client authentication. Implement self tests and a strong random number generator to reduce risk. Use a documented and strong key management process since breakdowns in this process can lead to compromise of the encryption keys.

Email

Email is a critical business application and used by almost everyone. Employees have their own corporate account or a shared corporate account. They also have personal email accounts that they may access with corporate computers. Email is a critical business tool for merchants and customers; however it also was developed decades ago without security in mind. Today, technologies such as Simple Mail Transfer Protocol (SMTP) and Post Office Protocol version 3 (POP3) are the underpinnings of our worldwide email system. SMTP is used to transport email messages between computers. POP3 servers receive the email messages and store them until a POP3 client logs in and downloads the emails.

When installing the SMTP service on a server, install all the latest security patches and keep them up-to-date, process all email in plain text not RTF or HTML and enable all vendor security precautions in the mail client. Use at least two reputable vendors' antivirus software packages running on the server that analyze all email traffic and attachments. Many times each antivirus software vendor will identify different vulnerabilities at different times.

When implementing a POP3 server be sure to install and maintain all vendor security patches and utilize SSL to protect logon credentials from POP3 clients. When installing a POP3 client on computer, be sure to set it to process all emails in plain text, not RTF or HTML since malicious code can be embedded in these formats. All POP3 clients should be maintained with all the most recent vendor security patches, have all security options enabled and use antivirus software.

Remote Management

Remote Desktop Protocol (RDP) and Simple Network Management Protocol (SNMP) are used to manage computers and devices on a network. RDP allows users to have an interactive desktop on another computer on a network. RDP is not completely secure and should be wrapped in SSH. When implementing RDP use the highest level of encryption, set session time limits, limit the number of sessions on the computer and set permissions for users and groups on the server. SNMP is used to monitor and manage devices on a TCP/IP network. SNMP version 3 is more secure than prior versions and should be implemented. SNMP authentication and session keys derivation should be implemented using HMAC SHA-1-96. Default community strings should be a combination of at least 8 alphanumeric and special characters. SNMP should be used with a security protocol such as SSL or SNMP over IPsec to protect management communication.

LAN Internet Protocols

LAN Internet protocols are used to manage internal TCP/IP networks and allow them to communicate on internal and external TCP/IP networks. These protocols include Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP) and Dynamic Host Configuration Protocol (DHCP). ARP is used to tie an IP address of a computer to its Media Access Control (MAC) address, the unique number on a network devices Ethernet adaptor. ARP allows computers to communicate across connected networks. When implementing ARP on a network use static ARP entries for the computer default gateway, which disables an attacker spoofing ARP messages and intercepting network traffic. Secure ARP is recommended since it incorporates digital signatures for integrity and authentication. ICMP messages are used to send error messages from the computer kernel level. These messages can be used by attackers who can discover information about computer hosts.

When implementing ICMP, disable ICMP responses from computers and block ICMP at the network firewall. IGMP is used efficiently broadcast TCP/IP data packets among computers on a network. When implementing IGMP, ensure that the latest vendor security patches are applied and maintained. DHCP is used to assign temporary IP addresses, netmask and default gateway to computers on a network. When implementing DHCP only use it for assigning and managing IP addresses. This limits an attacker implementing a rogue DHCP server which may compromise computers netmask and default gateway settings. These settings will need to be manually configured on the client computers.

Employees

Merchant employees are the first and last line of defense for the protection of sensitive data. Most data compromises originate from inside an organization. Having a detailed security policy that all employees are required to read goes a long way towards maintaining a secure environment. Security is everyone's job. Information security is just as critical as controlling the cash drawer. Today's criminals look for physical and technical vulnerability. All of the weaknesses described in this chapter are well known to the criminal community and do not require specialized skill to execute.

CHAPTER 8

POS CONNECTIVITY SECURITY

Cost Savings Bring Risk Too

A quiet revolution has occurred in the POS and debit card industry. Once embedded in proprietary, closed-end systems, POS devices and their processors often send authorization and other value-bearing transactions, along with card data, to other processors, their debit networks and their back offices. They use the same protocols and technology that power the Internet – the same ubiquitous method for identifying and routing data - the Internet Protocol (IP).

What Can Go Wrong?

POS PIN Pads sometimes link to Windows based hosts or other client server technology and rely on virtual “ports” or hooks into the application for monitoring, configuration and system management. Such ports and other IP based servers need to be logically secured, or even switched off, to prevent misuse and/or outside intrusion. Because the IP protocol broadcasts the existence of the machine, as well as its location and “willing” or open ingress ports, unauthorized individuals may seize the opportunity to:

- Take control of the host
- Introduce a rogue program, worm or virus
- Fail to detect an unauthorized device or application
- Capture cardholder data, PIN number and keystrokes
- Alter denials to approvals
- Disrupt traffic by introducing large amounts of data that cannot be processed (denial of service attack)

These risks may exist even though the PIN pad platforms of many POS host processors utilize “private circuits” to reach their processor or authorizing hosts. Although privately owned circuits may be used, the IP protocol is often used within the circuit or frame relay link to identify the PIN pad, its transaction gateway and back office link. Simply put, IP is so ubiquitous that the risk cannot be discounted. If only one component of your network or service provider’s network is compromised or disrupted, the POS host may become visible to hackers who wish to learn more about the network configuration and potential vulnerabilities.

Documenting Your Network Connections is a Vital First Step

Building secure POS connections starts with mapping your network and using network switches, routers, and VPSN to segment it. Internally, networks can host or provide centralized access to mission-critical applications and information, making secure access an organizational priority. Externally, networks integrate institution and third-party applications that grant customers and insiders access to their host systems that contain card data and POS terminal, wireless access points and POS PIN pads. These computer networks often extend connectivity far beyond the financial institution and its data center.

Dividing and Segmenting the Network is a Second Step

An effective approach to securing any network involves dividing the network into logical security domains. A logical security domain is a distinct part of a network with security policies that differ from other domains and perimeter controls enforcing access at a network level. The differences may be far broader than network controls, encompassing personnel, host, and other issues.

Before establishing security domains, POS processors and merchants should map and configure the network to identify and control all access points. Network configuration considerations could include the following actions:

- Identifying the various applications and systems accessed via the network,
- Identifying all access points to the network including various telecommunications channels ((for example, wireless, Ethernet, frame relay, dedicated lines, remote dial-up access, extranets, Internet),
- Mapping the internal and external connectivity between various network segments,
- Defining minimum access requirements for network services (for example, most often referenced as a network services access policy), and
- Determining the most appropriate network configuration to ensure adequate security and performance.

With a clear understanding of network connectivity, the POS processor or merchant can avoid introducing security vulnerabilities by minimizing access to less-trusted domains and employing encryption for less secure connections. Institutions can then determine the most effective deployment of protocols, filtering routers, firewalls, gateways, proxy servers, and/or physical isolation to restrict access.

Some applications and business processes may require complete segregation ((for example, no connectivity between web servers, wireless access points and retail locations). Others may restrict access by placing the services that must be accessed by each zone in their own security domain, commonly called a DMZ.

Security domains are bounded by perimeters. Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as DNS. The perimeter controls may exist on separate devices or be combined or consolidated on one or more devices.

Selecting Critical Filtering and Access Controls the Third Step

Designers of secure POS merchant networks need to leverage several tools for insulating their networks from intrusion and malware. These tools include:

- Firewalls
- DMZs
- Malicious code filtering outbound filtering
- Network intrusion prevention systems
- DNS placement
- Wireless security
- Securing remote access
- File authentication

Firewalls

A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).

POS processors and merchants have four primary firewall types from which to choose: packet filtering, stateful inspection, proxy servers, and application-level firewalls. Any product may have characteristics of one or more firewall types. The selection of firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the systems and data, and applications.

Typically, firewalls block or allow traffic based on rules configured by the administrator. Rule sets can be static or dynamic. A static rule set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is the result of coordinating a firewall and an IDS. For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address. The firewall, after ensuring the IP is not on a “white list”, creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.

Packet Filter Firewalls

Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet filtering capabilities.

Dynamic packet filtering incorporates stateful inspection primarily for performance benefits. Before re-examining every packet, the firewall checks each packet as it arrives to determine whether it is part of an existing connection. If it verifies that the packet belongs to an established connection, then it forwards the packet without subjecting it to the firewall rule set.

Stateful Inspection Firewalls

Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial “handshake” communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

Proxy Server Firewalls

Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices.

The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are the domain name server (DNS), Web server (HTTP), and mail (SMTP) server. Proxy servers frequently cache requests and responses, providing potential performance benefits.

Additionally, proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering. Web and email proxy servers, for example, are capable of filtering for potential malicious code and application-specific commands (see the “Malicious Code Filtering” section). They may implement antivirus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the security policy of the institutions.

Proxy servers are increasing in importance as protocols are tunneled through other protocols. For example, a protocol-aware proxy may be designed to allow Web server requests to port 80 of an external Web server, but disallow other protocols encapsulated in the port 80 requests.

Application-Level Firewalls

Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers. Application-level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

Firewall Services and Configuration

Firewalls may provide some additional safeguards:

- Network address translation (NAT)—NAT re-addresses outbound packets to mask the internal IP addresses of the network. Un-trusted networks see a different host IP address from the actual internal address. NAT allows an institution to hide the topology and address schemes of its trusted network from un-trusted networks.
- Dynamic host configuration protocol (DHCP)—DHCP assigns IP addresses to machines that will be subject to the security controls of the firewall.
- Virtual Private Network (VPN) gateways—A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways but not from the gateway to the terminating machines. Placement on the firewall, however, allows the firewall to inspect the traffic and perform access control, logging, and malicious code scanning.

Effective Use of DMZs and Firewalls is a Fourth Important Step

One possible firewall implementation is a DMZ, which is a neutral Internet accessible zone typically separated by two firewalls. One firewall is between the private network of the institution and the DMZ and then another firewall is between the DMZ and the outside public network. The DMZ constitutes one logical security domain, the outside public network is another security domain, and the internal network of the institution may be composed of one or more additional logical security domains.

An adequate and effectively managed firewall can ensure that computer systems of an institution are not directly accessible to any on the Internet.

Firewalls are an essential control for a POS processor or merchant with an Internet connection, and provide a means of protection against a variety of attacks. Firewalls should not be relied upon, however, to provide full protection from attacks. Institutions should complement firewalls with strong security policies and a range of other controls. In fact, firewalls are potentially vulnerable to attacks including:

- Spoofing trusted IP addresses,
- Denial of service by overloading the firewall with excessive requests or malformed packets,
- Sniffing of data that is being transmitted outside the network,
- Hostile code embedded in legitimate HTTP, SMTP, or other traffic that meet all firewall rules,
- Attacks on un-patched vulnerabilities in the firewall hardware or software,
- Attacks through flaws in the firewall design providing relatively easy access to data or services residing on firewall or proxy servers, and
- Attacks against computers and communications used for remote administration.

Financial institutions can reduce their vulnerability to these attacks through network configuration and design, sound implementation of its firewall architecture that includes multiple filter points, active firewall monitoring and management, and integrated security monitoring. In many cases, additional access controls within the operating system or application will provide an additional means of defense.

Given the importance of firewalls as a means of access control, good practices include:

- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit (see “Systems Development, Acquisition, and Maintenance”);
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic;
- Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed;
- Using NAT and split DNS to hide internal system names and addresses from external networks (split DNS uses two domain name servers, one to communicate outside the network, and the other to offer services inside the network);

- Using proxy connections for outbound HTTP connections;
- Filtering malicious code;
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks;
- Logging activity, with daily administrator review (see “Logging and Data Collection”);
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall (see “Security Monitoring”);
- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access;
- Limiting administrative access to few individuals; and
- Making changes only through well-administered change control procedures.

Malicious Code Filtering

Perimeters may contain proxy firewalls or other servers that act as a control point for Web browsing, email, P2P, and other communications. Those firewalls and servers frequently are used to enforce the institution’s security policy over incoming communications. Enforcement is through antivirus, anti-spyware, and anti-spam filtering, the blocking of downloading of executable files, and other actions. To the extent that filtering is done on a signature basis, frequent updating of the signatures may be required.

Outbound Filtering

Perimeter servers also serve to inspect outbound communications for compliance with the security policy of an institution. Perimeter routers and firewalls can be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers could be configured to identify and block customer data and other data that should not be transmitted outside the security domain.

Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (IPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads. They are similar to firewalls because they are located in the communications line, compare activity to preconfigured or preprogrammed decisions of what packets to pass or drop, and respond with pre-configured actions. The IPS units generally detect security events in a manner similar to IDS units and are subject to the same limitations.

After detection, however, the IPS unit may take actions beyond simple alerting to potential malicious activity and logging of packets. For example, the IPS unit may block traffic flows from the offending host. The ability to sever communications can be useful when the activity can clearly be identified as malicious. When the activity cannot be clearly identified, for example where a false positive may exist, IDS-like alerting commonly is preferable to blocking.

Although IPS units are access control devices, many implement a security model that is different from firewalls. Firewalls typically allow only the traffic necessary for business purposes, or only “known good” traffic. IPS units typically are configured to disallow traffic that triggers signatures, or “known bad” traffic, while allowing all else. However, IPS units can be configured to more closely mimic a device that allows only “known good” traffic.

IPS units also contain a “white list” of IP addresses that should never be blocked. The list helps ensure that an attacker cannot achieve a denial of service by spoofing the IP of a critical host.

DNS Placement

Effective protection of the DNS servers of a POS processor is critical to maintaining the security of the communications of an institution. Much of the protection is provided by host security (See the “Systems Development, Acquisition, and Maintenance” section of this booklet).

However, the placement of the DNS also is an important factor. The optimal placement is split DNS, where one firewalled DNS server serves public domain information to the outside and does not perform recursive queries, and a second DNS server, in an internal security domain and not the DMZ, performs recursive queries for internal users.

Wireless Security – Secure the Airwaves

Wireless networks are difficult to secure because they do not have a well-defined perimeter or well-defined access points. Unlike wired networks, unauthorized monitoring and denial of service attacks can be performed without a physical wire connection. Additionally, unauthorized devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices.

To mitigate those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. If a POS processor or merchant uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls.

Examples of additional controls may include one or more of the following:

- If possible, the wireless network supporting the POS devices should authenticate devices that wish to attach to it through machine names, also known as MAC addresses. MAC addresses are specific logical addresses found at layer 3 of the TCP/IP message stack. When setting up the device, the system administrator would identify PCs or other devices that have legitimate reasons for wirelessly connecting to the POS network. When such access is requested, the wireless access point connected to your POS network will only let in access requests with MAC addresses from approved devices.
- When setting up the wireless access point, do not broadcast your system identifier known as the SSID. If hackers cannot see your system from their wireless PC, they will not be able to log on to your wireless access point.
- Treating wireless networks as un-trusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment;
- Using end-to-end encryption in addition to the encryption provided by the wireless connection.
- Using strong authentication and configuration controls at the access point and on all clients.
- Using an application server and dumb terminals.
- Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference.
- Monitoring and responding to unauthorized wireless access points and clients.

Securing Remote Access to the POS Network: The Fifth Step

Remote access to the systems of a POS processor or merchant provides an attacker with the opportunity to subvert the institution's systems from outside the physical security perimeter. Accordingly, management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices should be strictly controlled. Good controls for remote access include the following actions:

- Disallow remote access by policy and practice unless a compelling business justification exists.
- Require management approval for remote access.
- Regularly review remote access approvals and rescind those that no longer have a compelling business justification.
- Appropriately configure remote access devices.

- Appropriately secure remote access devices against malware (see the “Malicious Code Filtering” section).
- Appropriately and in a timely manner patch, update, and maintain all software on remote access devices.
- Use encryption to protect communications between the access device and the institution and to protect sensitive data residing on the access device.
- Periodically audit the access device configurations and patch levels.
- Use VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution.
- Log remote access communications, analyze them in a timely manner, and follow up on anomalies.
- Centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring.
- Log and monitor the date, time, user, user location, duration, and purpose for all remote access.
- Require a two-factor authentication process for remote access ((for example, PIN-based token card with a one-time random password generator, or token-based PKI).
- Implement controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the following controls:
 - Restrict the use of the access device by policy and configuration
 - Require two-factor user authentication
 - Require authentication of the access device
 - Ascertain the trustworthiness of the access device before granting access
 - Log and review all activities (for example, keystrokes)
- If remote access is through modems:
 - Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorized external requests, and disable the modem immediately when the requested purpose is completed.
 - Configure modems not to answer inbound calls, if modems are for outbound use only.

- Use automated callback features so the modems only call one number (although this is subject to call forwarding schemes).
- Install a modem bank where the outside number to the modems uses a different prefix than internal numbers and does not respond to incoming calls.

Securing File Downloads

POS merchant processors should implement security procedures to reduce the risk of accepting unauthorized data transmissions to their hosts and POS devices. Digital file signing techniques to verify the authenticity of a given file should be applied *before* it can be executed on a terminal or PIN pad. For a file to be authenticated, it must be digitally “signed” by an authorized party, proving that the file is an original that has not been changed from the date it was approved.

This is done by comparing the signature in a file against a copy of the signature, using public/private key verification. The actual file signing takes place with the help of a smart card-based file signing tool. This technique establishes a “chain of trust,” whereby the digital certificate that is used to verify the file is itself verified by the next higher digital certificate in the chain. This process continues all the way up to the “trusted root” certificate that the certificate authority or manufacturer should securely load into the terminal at its manufacturing facility. If all the information is validated; the application is accepted and is ready to run. If discrepancies are found, the software download is rejected and is either erased or not allowed to execute on the terminal.

CHAPTER 9

POS DECOMMISSIONING SECURITY

Introduction to POS Decommissioning & Disposal Recommendations

Point of Sale Devices (POS) are in proliferation around the world (estimated at 20 million installed units). Initially these were relatively simple “carbon copy” machines using signature verification by the sales assistants. Modern POS devices are at minimum card swipe readers using magnetic stripe verification, but increasingly, they are Chip & PIN readers using PIN verification.

It has been noted by the criminal elements that the card reader decodes the customer card information, and, where appropriate, the PIN data contained on the card. This has led to criminals targeting the card reader for both skimming and false recording of customer data. Much of this activity can only be achieved after detailed inspection and availability of a POS device for reverse engineering.

The need for disposal of POS devices results from replacement due to technology obsolescence, faults which are beyond economical repair, and supplier change. All units for disposal are subject to requirements for correct environmental disposal at end of life.

Resale of Equipment

POS equipment may be on lease or sold to a customer. Where the product is on lease, then it should be returned to the supplier on completion of the lease period. The **supplier** then has the full obligation for correct disposal.

If units are sold to a customer, when new technology becomes available the **customer** will have a requirement to dispose of obsolete units. This may occur either as a trade-in to the new supplier, or by the customer selling directly to a third party.

The selling to a third party leaves an obligation on the **seller** to ensure the units are to a bone fide organization, and are not sold without a sales record, model, serial number, date, end user identification, overseas license documentation (if required), and a liability transfer statement regarding final disposal instructions together with references to appropriate recommendations.

POS Security Disposal Recommendations

The disposal of POS devices needs to take account of any existing legislation, but at a minimum should take account of the following guidelines:

- a) Only regulated companies for the disposal and destruction of POS materials should be used
- b) Collection and storage (awaiting disposal) should be by regulated companies.
- c) Material to be destroyed should be classified, including embedded software, chip/magnetic stripe card readers, components and other relevant hardware.
- d) Any hazardous waste should be subject to disposal in accordance with existing legislation applicable to the destruction/disposal of hazardous waste (see section below on environmental guidelines).
- e) Destruction shall mean reduction in size such that, as much as practicable, material becomes unreadable, illegible, and unable to be reconstructed.
- f) Methods of destruction include shredding (reduction by mechanical means to a regulated size) and disintegration (reduce by mechanical means to a regulated size less than that achievable by shredding).
- g) Where feasible, end products consisting of recyclable material (for example, metal or plastics should be recycled (see below).

Federal Trade Commission Disposal Rule (16 CFR Part 682) states the need to remove all personal and financial information from any machine for disposal. Memories should be cleaned of all installed programs and memory/processor hardware should be destroyed by physical destruction (Compressor or Shredder).

- h) End destroyed product should, where practicable, be recycled. Where the end product cannot be recycled, the environmental impact, cost and convenience of other methods of waste disposal (for example, incineration) should be taken into account. Landfill should only be used were no other method of disposal is practicable. (see section below on Environmental Disposal Recommendations and Guidelines).

POS Environmental Disposal Recommendations and Guidelines

The WEEE Directive (Waste Electrical and Electronic Equipment Directive) is intended to introduce EU legislation, which places ownership for environmental disposal of products on the Manufacturer (irrespective of location if goods are sold/used in EU member states). This is because the manufacturer is/should be, aware of the materials used in the manufacturing process, and is therefore responsible for their environmental impact.

It is intended to ensure manufacturers are environmentally cognizant, and take materials into account for future designs and development.

A summary of the key sections of the EU WEEE Directive as applicable to POS disposal are given here:

- a) Applicability – Applies to all EU states for products and producers irrespective of distance or selling techniques. Obligations for producers and distributors should take the same form and be subject to the same enforcement to ensure that costs are borne by all parties.
- b) The Directive covers all electrical and electronic goods used by consumers or for professional use in contract with the WEEE and associated legislation.
- c) Objective of the WEEE is to encourage producer responsibility to design for facilitating repair, upgrading, reusing, disassembly and recycling of useable materials.
 - EU Member states will be responsible for implementing the WEEE Directive.
 - Information on component and material identification to be provided by the equipment producers to facilitate the WEEE.
 - Inspection and monitoring for WEEE directive compliance to be established at member state level.
 - Product design to facilitate WEEE directives should be encouraged by member States and should take into account and facilitate dismantling and recovery; in particular the recycling and reuse of WEEE their components and materials.
 - When supplying new product, manufacturers and distributors are responsible for the provision of waste return free of charge on a one-for-one basis.
 - Equipment for disposal that is exported out of the EU can only be exempt from the WEEE directive if the export disposal instructions can be proved to be equivalent to the instructions in the WEEE directive.
 - Financing for the costs, collection, treatment, recovery and environmentally sound disposal for equipment is the responsibility of the producer of the equipment.
 - Penalties for non compliance – Member states shall determine penalties applicable to breaches of the national provisions pursuant to the WEEE directive which shall be effective, proportionate, and dissuasive.

- Selective treatment of materials such as:
 - Batteries
 - Mercury containing components
 - Polychlorinated Biphenyls (PCB) and Polychlorinated terphenyls (PCT)
 - Printed Circuit Boards if the surface area is greater than 10 sq cms
 - External electrical cables
 - Liquid crystal displays (subject to size)
 - Electrolyte capacitors

A full list of items can be found in Annex 11 of the WEEE directive.

The U.S. EPA (Environmental Protection Agency) has issued simplified guidelines as summarized below:

“Manufacturers or their designees, are to develop, finance, and implement a waste recovery system for the collection, handling, transportation, processing, recovery, reuse, and recycling of the devices sold by the producer.

Manufacturers will have the option of foregoing the collection and recycling by paying a fee to cover the full cost of collection and recycling of every device sold (currently estimated between \$5-\$10 per unit)”

The above guidelines are at various stages of implementation by each state, throughout the United States, with some having introduced legislation, others signed into law, or in committee. It should be noted that were U.S. Manufacturers sell into the EU states they are also are responsible for meeting the WEEE Directive obligations.

Relevant References

- a) WEEE (Directive on Waste Electrical and Electronic Equipment)
- b) BS 8470 (Disposal of Confidential Material [Hardware, Software & Printed])
- c) READ (Recycling Electronic and Asset Disposition)
- d) Federal Trade Commission Dispersal Rules (16 CFR Part 682)
- e) SWANA (Solid Waste Association of North America)
- f) NWSMA (National Solid Waste Management Association)
- g) International Association of Electronic Recyclers
- h) EPA (US Environmental Protection Agency) Guidelines

- i) RCRA (Resource Conservation and Recovery Act) Federal Environmental Law
- j) The Consumer Educational Institute (CEI) is a US program developed by the Environmental Issues Council of the Electronic Industries Alliance (EIA). The purpose is to inform consumers about recycling and reuse for used electronics
- k) US Technology/Recycling Computer and related Equipment Plan.

ACKNOWLEDGMENTS

ATMIA would like to thank MasterCard Worldwide for providing their excellent POS Terminal Security Program – Security Best Practices document. In addition, the Debit Council would like to acknowledge invaluable contributions and support from the following individuals:

Mike Urban, Fair Isaac

Bruce Sussman, NYCE

Lyle Elias, EFT Data

Marilyn Kilcrease, Creative Card Solutions

Peter Kulik, Fifth Third Bank

Sandeep Dhameja

Doug Manchester, Verifone

Alicia Gaff, RBS Lynk (Technical Editor)

Susan Kohl, RBS Lynk

Dianne DeFrancesco, RBS Lynk (Technical Editor)

Scott Spiker, Hypercom

Graham McKay, ATMIA Europe

Mike Lee, ATMIA

Suzanne Lynch, MasterCard Worldwide

Leland Englebardt, MasterCard Worldwide

Julie Shaw, Pulse- EFT

John Spence, Ingenico

Jan Mardin

DISCLAIMER

This manual has been developed in furtherance of GASA's and ATMIA's nonprofit purposes. The information contained in this manual is intended to identify Best Practices in the POS industry, but is not a standard for best practice. Therefore, use, reference to, or review of the material in the manual does not and cannot guarantee the elimination of risk inherent in the delivery of POS services and should not be used as a standard or mandatory requirement for conducting business in the ATM and POS industry. It is recommended that the manual be used as guidance in connection with the implementation of Best Practices, but not as a substitute for diligent review and analysis regarding application of the Best Practices.

GASA and ATMIA have taken reasonable measures to develop the manual and recommended Best Practices in a fair, reasonable, open, and objective manner. However, GASA and ATMIA make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information being provided. In addition, views of appropriate practices may change over time and errors or mistakes may exist or be discovered in this material. As such, inclusion of material in this manual does not constitute a guarantee, warranty, or endorsement by GASA or ATMIA regarding the views, methodologies, or preferences for implementing the Best Practices. Further, neither ATMIA nor GASA nor its officers, directors, members, authors, or agents shall be liable for any loss, damage, or claim with respect to any such information or advice being provided. All such liabilities, including direct, special, indirect, or consequential damages, are expressly disclaimed and excluded.