Issuer PIN Security Guidelines

November 2010

Issuer PIN Security Guidelines

November 2010

Table of Contents

Using This Document

Purpose

This manual provides guidelines for PIN security in the issuer domain during:

- Use of issuer approved[1] devices for PIN entry during transactions requiring PIN entry, for example non POS/ATM or 'On-Us' ATM transactions.
- Cardholder PIN management.

The intent of these guidelines is to manage the exposure of PINs and associated data (processed during the types of transaction within the scope of this document) that could be used to clone cardholder payment devices for use in any payment channel.

These guidelines represent best practice for issuer PIN management unless business needs dictate otherwise.

Under these guidelines, issuer PIN security management is at the issuer's own risk.

Acquirer PIN security requirements for the secure management, processing, and transmission of PINs during online and offline payment card transaction processing at ATMs, and attended and unattended point-of-sale (POS) terminals are provided in the PCI PIN Security Requirements. Cardholder PIN entry in the acquirer domain should be performed using PED/EPPs in accordance with payment-system brand requirements that relate to the PCI PTS Program

This manual is designed to provide PIN security guidelines for all payment accounts that use a PIN, including those associated with magnetic stripe cards, chip cards, 'hybrid' cards that incorporate both a magnetic stripe and a chip or any other cardholder payment device form factor.

These guidelines were derived from existing Visa and MasterCard documentation and finalized in this version by representatives of the two payment-system brands.

Payment-system brand rules that relate to topics in this document supersede any guidelines on those topics.

[1] A device, possibly provided by the issuer but not necessarily, whose use for cardholder PIN entry is permitted under conditions specified by the issuer.

Scope

The scope of this document extends to system components (for example service providers, networks, servers, hosts, applications, processes and personnel) which are used to exchange PIN-related data. The PIN Guidelines in this document encompass PIN security within any one system or sub-system and between systems.

These guidelines are targeted at PIN protection during PIN processing in the issuer security domain.

PIN processing of interchange transactions is covered by the PCI PIN Security Requirements.

Payment applications impacted by these guidelines

This document applies to any PIN used as a CVM in the issuer security domain with a payment-system brand application, irrespective of the cardholder payment device on which that application resides.

Terminology

A PIN (Personal Identification Number) is a four to twelve digit number known by a cardholder and used to authenticate the cardholder to the card-issuing bank (or to the cardholder's ICC).

The transaction PIN is the PIN entered by the cardholder during a payment transaction. (Unless otherwise stated, any reference to a PIN throughout this document implies the transaction PIN.)

The online PIN is the transaction PIN used to verify the cardholder online.

The offline PIN is the transaction PIN used with an ICC to verify the cardholder offline.

The reference PIN is a stored, or derived PIN value used by the issuer to verify the transaction PIN. If stored in an ICC it may or may not be equal to the online PIN.

The PIN may also be verified using a PIN verification value or a PIN offset either transmitted with the transaction PIN or stored at the issuer host.

PIN Verification

PIN verification may be of two types: online and offline.

The two verification processes operate in the following manner:

- **Online verification:** The PIN entered by the cardholder is transmitted to the issuer (or its designated service provider) for verification, together with the card details (possibly read from the magnetic stripe or IC of the payment card or manually entered). Transmission is typically via the merchant acquirer or financial institution; or a third party service provider. The precise method used to verify the PIN is also in the scope of this document. The PIN verification algorithm is selected by the issuer.

- **Offline verification:** Depending upon the mutual capabilities of the ICC and the ICC reader, the PIN entered by the cardholder is either transferred to the ICC in cleartext form or, encrypted under the ICC's public key used for PIN encipherment. The PIN must be input to the ICC using ISO PIN block format 2 . Whether in cleartext form or encrypted, the ICC has an internal method for verifying the PIN (for example as per EMV). The ICC indicates the result of the PIN verification to the terminal. PIN verification can also be performed by the issuer during the transaction (if it is sent online) or after the transaction by inspection of the relevant chip data elements.

The PIN associated with a magnetic stripe card can only be verified by the issuer's systems, as the card cannot perform any computations itself.

The PIN associated with an ICC can be verified by the issuer's systems (as with a magnetic stripe card) or offline by the ICC itself.

There are important differences between the two types of verification and what they achieve in terms of security:

- Following a successful online PIN verification, the merchant will be given an assurance via the acquirer that the PIN is valid for the card details. There is no assurance, however, that the physical card itself is valid – in the case of a magnetic stripe card it may be a cloned device manufactured using valid account details.
- Following a successful offline PIN verification (with no online authorization); the merchant has a lower level of assurance than for on-line verification, namely: if the ICC is valid and its response has not been modified, then the PIN is valid for this ICC. This is because it may be possible to program a counterfeit ICC to respond to the terminal as if the valid PIN had been entered. However if dynamic offline CAM[2] is also performed, the assurance that the card and PIN are valid is restored as for the online case.

ICCs are commonly hybrid cards (i.e. cards equipped with both an IC and a magnetic stripe) that can be used with magnetic stripe only terminals, ICC only terminals, or with dual mode terminals to ensure their interoperability with existing payment acceptance devices,

Issuer Approved PIN Entry

This document also defines security guidelines for issuer approved devices for PIN entry where:

- PIN entry is performed using a personal or private cardholder device (for example, remote transactions using personal computers, set-top boxes, landline or mobile phones),
- PIN entry is performed using a public device that is not under the control of the issuer (for example, an e-commerce transaction using a public Internet kiosk).

[2] EMV supports two types of dynamic offline CAM: DDA and CDA. Both types protect against counterfeit ICCs by means of a challenge-response mechanism between terminal and card; however CDA additionally protects against the risk of a wedge device being inserted between the terminal and card and modifying the messages sent between them, e.g. to mislead the terminal regarding offline PIN verification status.

Physical security requirements need not be as stringent on a personal device for PIN entry, as on an acquirer controlled PED/EPP, because the user of a personal device has a higher degree of control over the physical integrity of the device and can typically detect when the device is stolen, substituted or physically tampered with. However, such devices may be ill equipped against logical attacks which may go undetected by the user.

A public device used for PIN entry may be difficult to police both physically and logically. The use of such devices depends upon the level of risk that the issuer is willing to accept.

PIN Lifecycle Reference

The PIN management guidelines in this document refer to the following processes.

Process	Process Description	
PIN Creation	Generation of the PIN, card magnetic stripe personalization, ICC personalization (if applicable), load to issuer authorization systems.	
	PIN selection	Cardholder self-selection of PIN.
PIN Transmission	Any transmission of PINs: • between issuer approved PIN handling devices, • to and from cardholders.	
PIN Storage	Protection of PIN-related data by issuers, issuer approved PIN handling devices and cardholders	
PIN Processing	All processing of PINs within a PIN-handling device.	
	Online PIN verification	Online verification of the cardholder PIN.
PIN handling device management	Deployment, usage and decommissioning of equipment used to process and store PINs.	
PIN related Key Management	Management of cryptographic keys for secure PIN creation, storage, processing, transmission and verification	
Cardholder authentication	Process by which the cardholder supplies credentials to a system to access PIN management functionality	
PIN advice	Notification of the PIN to the cardholder.	
PIN change	Cardholder or issuer re-selection of PIN.	
Additional PIN management functions	Any other functionality required by issuers to manage their PINs	

General PIN Management Guidelines

The following guidelines apply to all aspects of the PIN management system. Issuers should:

- Ensure that any exposed data or credentials required for PIN management do not permit personalization of undetectable, unauthorized cardholder payment devices that can be used to make any payment with or without PIN as a CVM.

  For example when ICC or magnetic stripe data is processed it is vulnerable to the following:

  - Processed chip data (track 2 equivalent data without a distinguishing chip CVC/iCVV) can be used to create a magnetic stripe card clone. If the PIN is also available the clone may be used, undetected by the issuer host systems, for example at an ATM that does not accept ICCs.
  - Processed chip data can be used to create a ICC (without secret issuer keys). Transaction routing to a third party stand-in provider may result in transaction authorization if stand-in does not share issuer keys.
  - Processed chip data or magnetic stripe data can be used to generate CNP credentials.
  - Processed magnetic stripe data can be used to create a magnetic stripe card clone. If the PIN is also available the clone may be used, undetected by the issuer host systems, at an ATM.
- Confirm that the security checks performed on transaction data by their authorization host will detect when a transaction is from an unauthorized cardholder payment device for example:
  - The application should detect when a HSM fails to verify a chip card verification code that is provided during a magnetic stripe transaction.
  - Issuers should verify the presence of the magnetic stripe during magnetic stripe transactions by using the card verification code, i.e. not solely rely upon the verification of the online PIN and correctness of the PAN.
  - Issuers should decline ATM and POS cash back transactions which result in a card verification code failure.
  - Issuers should validate all of the key information contained in the authorization request. These elements may include cardholder name, expiration date, PIN verification data and other discretionary data elements.
  - Issuers should review and update velocity monitoring and neural network parameters for PIN transactions for example:
    - Excessive PIN attempts
    - Excessive PIN transactions
    - Excessive cashback or quasi-cash transactions
    - Separate daily/multi-day quasi-cash velocity parameters
    - Separate daily/multi-day cashback velocity parameters
    - High-risk countries

- Reduce PIN management as a target for fraudsters by maintaining separation of the PIN from associated account data used for payment transaction processing throughout the PIN management processes.
- Ensure that PINs are protected during processing, transmission and storage by one or more of the following:
  - Provision of physical protection
  - Encryption of the PIN
  - Use of separate HSMs for Issuer vs. Acquirer functionality
  - Use of an encrypted reference or control number to indirectly link the PIN to the PAN when the two items of data must be transmitted separately.
  - Issuers should ensure that their PIN management system prevents the PIN from being stored wherever it is received while under issuer responsibility. PIN mailers, SMS messages and emails are vulnerable and their content should be constructed to meet the PIN Generation, General Guidelines section.
- Conduct employee monitoring with respect to accessing cardholder data. Routine monitoring can help determine if employees are accessing cardholder records when there is no need to do so, for example accessing an unusual amount of cardholder records, or asking for cardholders' PINs.
- Provide guidance on safe PIN management to cardholders when the account is first opened, and at least annually, for example:
  - Never share your PIN with anyone.
  - Select a PIN that cannot be easily guessed (i.e., do not use birth date, partial account numbers, sequential numbers like 1234, or repeated values such as 1111).
  - Memorize your PIN. Do not write it down on your card or keep it on a piece of paper in your wallet.
  - Do not use your PIN as a password for other bank and non-bank services.
  - Be aware of others nearby when entering your PIN at an ATM or point of sale.
  - Check your monthly statements for unauthorized charges
- Regularly insert a PIN security reminder into cardholder statements and promote cardholder awareness of 'phishing' and other social engineering attacks.
- Issuers, member/client service providers and vendors providing any PIN management service should refer to brands for any mandates that apply to the service.

PIN Fraud Mitigations

- Apply risk factors to ATM withdrawal limit assignments:
  - Establish an expanded range of higher POS spending and ATM withdrawal limit tiers in combination with an ongoing limit upgrade program that is aligned with customer risk, as well as deposit classification/value. This strategy can promote higher penetration, spending, and usage for more credit-worthy customers, while minimizing risk exposure.
  - Review requests for higher ATM withdrawal limits at an individual cardholder level. Customer demand for higher ATM withdrawal limits is relatively small and should be satisfied by permitting individually-raised ATM withdrawal limits on a case-by-case basis.
- Apply cashback amounts to the ATM withdrawal limit. The cashback portion of a POS PIN transaction should always be applied toward the cardholder ATM withdrawal limit.
- Ensure that quasi-cash is categorized as cash and applied to the ATM withdrawal limit. The total amount of a quasi-cash transaction should also be applied to the ATM withdrawal limit.

Abbreviations

Abbreviation	Description
ANSI	American National Standards Institute
ATM	Automated Teller Machine
AVR	Automated Voice Response
AVS	Address Verification System
BIN	Bank Identification Number
CAM	Card Authentication Method
CAP	Chip Authentication Program
CAST	Compliance Assessment Security Testing
CNP	Card Not Present
CVC	Card Validation Code
CVM	Cardholder Verification Method
CVV	Card Verification Value
DES	Data Encryption Standard
DNS	Domain Name Server
DSS	Data Security Standard

Abbreviation	Description
DTMF	Dual tone multi frequency
EMV	the jointly agreed specifications for ICC-terminal operation
FIPS	Federal Information Processing Standards
GSM	Global System for Mobile
HSM	Hardware Security Module
IC Card / ICC	Integrated Circuit Card (same as smart card)
ISO	International Standards Organization
IFD	Interface Device
IVR	Interactive Voice Response
IMSI	International Mobile Subscriber identity
LAN	Local Area Network
MAC	Message Authentication Code
MCC	Merchant Category Code.
MITB	Man In The Browser
MITM	Man In The Middle
MO/TO	Mail order Telephone order
MSP	Member Service Provider
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
PAN	Primary Account Number
PC	Personal Computer
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
POI	Point of Interaction
POS	Point-of-Sale
PSD	Physically Secure Device

Abbreviation	Description
PSTN	Public Switched Telephone Network
P2P	Person to Person
PVV	PIN Verification Value
RF	Radio Frequency
RSA	Rivest, Shamir and Adleman (an asymmetric encryption algorithm, named after its inventors)
SCD	Secure Cryptographic Device (as defined in ISO 13491-1)
SIM	Subscriber Identification Module
SMS	Short Message Service
SSL/TLS	Secure Socket Layer/ Transport Layer Security
TDES	Triple DES
TPP	Third Party Provider
UTC	Coordinated Universal Time
WAN	Wide Area Network

Terminology

The following table provides definitions of the key terms used in this manual.

Term	Definition
Account Data	(PCI definition) At a minimum, account data contains the full PAN and (if present) any elements of sensitive authentication data. The following are also considered to be account data if sent in conjunction with the PAN: cardholder name, expiration date or service code.
Account holder	See cardholder.
Account issuer	The entity with which the cardholder has an account used to make payments. For single application cards, this is the same as the card issuer.
Associated data	All data associated with a PIN, including cardholder data. (See Cardholder Data)
Authenticity	The property of data or an entity that identifies origin.
Best practice	Security techniques that reduce risk at a practical cost.
Call center	A facility for managing telephone requests.

Term	Definition
Cardholder	The individual authorized by the issuer to use a PIN to identify him or herself in order to use a particular payment account. Such an individual is issued with a payment device used for the account.
Cardholder Data	All personally identifiable data about the cardholder/issuer relationship including, account data, PIN, expiration date, issuer data, electronic data gathered by a merchant during a transaction, addresses, telephone numbers, and information used for electronic access to PIN management functionality. (see also Associated Data)
Cardholder Payment Device	A physical device that interacts with a POI. A magnetic stripe card is an example. A mobile cardholder payment device may contain one or more payment accounts
Functionally Secure Device	A device that provides logical security so that the device can be compromised only by physical means.
Hardware Security Module	A hardware device that, when operated in its intended manner and environment, cannot be successfully penetrated to disclose or modify all or part of any secret or private cryptographic key or PIN resident within the device. This may require the provision of adequate tamper responsiveness facilities.
IMSI Grabber	A mechanism used to intercept wireless communication data between a mobile phone and the mobile operator base station.
Integrity	The property of data that identifies unauthorized modification.
Interchange Environment	The exchange of transaction data between acquirers and issuers in accordance with payment-system brand rules
Interface Device (IFD)	A device that can communicate directly with a ICC. In a POS terminal, the device that houses the ICC reader.
Intermediate processing networks	Any intermediate network used to transport PIN data that is not under the control of the issuer.
Issuer	The entity that issues payment applications to cardholders. For single application cards, this is the entity with which the cardholder has an account used to make payments. For multi-application IC cards, the card issuer might not be the entity with which the cardholder has an account used to make payments. In this case, that entity would be the 'application provider'. Note that Program Services may be performed by a TPP or MSP on behalf of an issuer.

Term	Definition
Issuer Approved device for PIN entry	A device provided by the issuer for cardholder PIN entry under conditions specified by the issuer or A device, not necessarily provided by the issuer, whose use is permitted for cardholder PIN entry under conditions specified by the issuer.
Issuer host database	Issuer database containing sensitive cardholder data in enciphered form.
Issuer network	Card issuer dedicated network defined by a specific security domain, may be WAN or LAN.
IVR server systems	Cardholder-facing voice recognition system that parses DTMF tones into data.
Keystroke Logger	A method of capturing and recording user input for example from a PC keyboard.
MITM attack	An attack based on active eavesdropping where two connected parties think they are communicating only to one another whereas they are each actually connected to an interceptor who can read and modify traffic as it is relayed between the two parties.
MIDlet	Java application conforming to the Java 2 Micro Edition Mobile Information Device Profile (J2ME MIDP). Typically targetted for use on a mobile phone..
Mobile device for personal PIN entry	A mobile device provided by the issuer for cardholder PIN entry under conditions specified by the issuer or a mobile device, not necessarily provided by the issuer, whose use is permitted for cardholder PIN entry under conditions specified by the issuer.
Off-line PIN	The PIN entered by the cardholder for off-line PIN verification.
Over the air (OTA) personalization	The transfer of personalization data to a mobile cardholder payment device via some form of Radio Frequency transmission – typically using the cellular radio network to which that device is registered.
Payment Account	A credit, debit or stored value account used to make payments.
Payment System Environment	The conditions that accomplish the legitimate transfer of money.

Term	Definition
Phishing	The use of social engineering in an electronic communication to gain unauthorized access to private personal and financial information.
PIN concentrator	The cardholder facing functional unit which processes a number of channels containing PIN and associated data to/ from cardholders, e.g. a web server, IVR server, mail server or SMS server and concentrates these into fewer channels for subsequent processing. The PIN concentrator provides an interface between the insecure domain occupied by the cardholder and a secure domain provided by the issuer or the issuer service providers.
PIN Entry Device (PED)	Any device under merchant or acquirer control into which a cardholder can enter a PIN. PIN entry is performed by means of a PIN pad that is part of the PED. Add PCI PTS link for list of approved devices
PIN-handling device	Any device that has access to cleartext PINs for one or more cardholder accounts (either for PIN entry or PIN notification) including HSMs used for PIN translation or verification.
PIN-handling system	The set of all interconnected PIN-handling devices.
PIN integrity	The integrity of the relationship between the PIN and associated data such as cardholder account data or transaction information.
PIN Offset	The difference between the cardholder's selected or assigned PIN and a derived PIN based on a specific algorithm that is applied against the primary account number (PAN)...
PIN pad	A numeric or alpha-numeric keypad into which cardholders type PINs.
PIN Processing	Manipulation of PIN data within a PIN-handling device.
PIN storage device	A PIN-handling device that stores a PIN for longer than is necessary to process it (either for secure transfer to another device or for the purposes of PIN verification).
PIN Transaction	Any transaction that requires the use of the PIN whether for PIN management or as a CVM for payment transactions.
PIN Verification Value	A value that enables an issuer to validate the cardholder identity when making a comparison with the PIN and PAN
Poisoned DNS cache	A means for providing false domain name information to a domain name server, for example causing cardholders to link to a fraudulent website even when the correct website address is entered by the cardholder.

Term	Definition
POS Device	Any device that participates in transaction processing at the point of sale (by processing, storing, or forwarding transaction, card, and cardholder data)
Program Service(s)	Service(s) to support an Issuer or an Acquirer's activity.
Reference PIN	A value used to verify a transaction PIN by an issuer, either online or offline.
Server-based Payment Application	A payment application that is accessed remotely, for example using a mobile phone/and or a web interface to enter authentication credentials to enable a money transfer.
Root kit	A program for obtaining unauthorized control of a system.
Secure Cryptographic Device (SCD)	A physically and logically protected hardware device that provides a set of cryptographic services (see ISO 13491).
Secure mailer	A method for secure transmission of printed sensitive data using tamper evident packaging, i.e. unauthorized tampering is evident to the intended recipient.
Sensitive cardholder data	Cardholder data required for PIN CVM, CNP CAM, ATM/ POS CAM or PIN management functionality.
Smart card	A device with an embedded integrated circuit capable of processing data.
SMS server system	A system used to convert authorized PIN management messages into SMS messages for transmission to a mobile which is authorized by the issuer.
SMSishing	Use of social engineering via a spoofed SMS message to gain unauthorized access to private personal and financial information.
Sniffer	Hardware or software that can intercept/analyze all or part of a network's traffic.
Tamper-evident device	A device with the special property that, if the device is compromised or substituted, this will be evident to any subsequent user. The tamper evidence afforded by a device will depend on device management procedures and operating environment.
Tamper-resistant device	A device that offers a measure of physical protection for the integrity of the device itself, and offers protection for the confidentiality and integrity of stored data.
Tamper-responsive device	A device that has the means to detect attempts to compromise its physical security, and will take actions if such attempts are detected. This will involve erasing stored information and/or displaying or sounding alarms.

Term	Definition
Terminal	A device or collection of devices used at the point-of-interaction to perform a payment card transaction. For a point-of-sale (POS) terminal, it typically includes the IFD, the PED, the magnetic stripe reader, and the POS device. In some POS configurations, it may also include the merchant host computer.
Transaction PIN	The PIN value entered by the cardholder as a CVM.
Two-factor authentication	An authentication mechanism that requires two credentials for example -something possessed by the cardholder (a cardholder payment device) and something known by the cardholder (a passcode or password).
Vishing	Use of social engineering and caller ID spoofing over VOIP to gain unauthorized access to private personal and financial information.
Web server systems	A computer that hosts a web application for an issuer, serving web page requests from browsers. The application: • authenticates the user • accepts PIN data input via a keyboard (or some other peripheral device connected to the PC) and converts it into data used for PIN management at issuer host. • delivers authorized PIN or cardholder account data to a PC screen from data used for PIN management at issuer host.

Related Standards

The following standards (as published) relate to information in this document.

1. American National Standards Institute (ANSI) X9.65: Triple Data Encryption Algorithm
2. ANSI X9.24 Banking – Retail Financial Services Symmetric Key Management
3. ANSI X9.42: Public Key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
4. ANSI X9.52: Triple Data Encryption Algorithm: Modes of Operation
5. Federal Information Processing Standards (FIPS) PUB 140 : Security Requirements for Cryptographic Modules
6. EMV Integrated Circuit Card Specification for Payment Systems (as published)
7. International Organization for Standardization (ISO) 9564: Personal Identification Number Management and Security
8. ISO/IEC 11568: Banking—Key Management (Retail)
9. ISO/IEC 11770: Information Technology—Security Techniques—Key Management

10. ISO/IEC 13491: Banking—Secure Cryptographic Devices (Retail)
11. ISO/IEC 18031: Information Technology—Security Techniques—Random bit generation
12. ISO TR 14742: Recommendations on Cryptographic Algorithms and their use.
13. ISO TR19038: Guidelines on Triple DES Modes of Operation
14. National Institute of Standards and Technology (NIST) Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
15. National Institute of Standards and Technology (NIST) Draft Publication 800-131: Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths
16. PCI SSC: PCI DSS.
17. PCI SSC: PCI PTS HSM Security Requirements
18. PCI SSC: PCI PTS POI Security Requirements

Guidelines for Issuer Approved Devices Used for PIN Entry

Objective

Applications that use an issuer approved device for PIN entry in the issuer security domain should restrict availability of PINs and related processed account data.

Threats

- The PIN and associated account data processed in such a device are vulnerable to eavesdropping which may arise if the device used for PIN entry has been compromised in any way, either by physical tampering or by execution of malicious software.
- Issuer host systems may not check for the presence of a magnetic stripe during a magnetic stripe transaction authorization. For example. authorization may rely solely on online PIN verification and correctness of the submitted PAN. Thus, cross-contamination of magnetic stripe payment transaction technology may be enabled through PIN management technology, i.e. Issuer PIN management may enable a magstripe clone to be created without the full magstripe present because the issuer does not perform sufficient security checking. .

  See General PIN management guidelines section for additional guidance for validating the presence of an authorised cardholder payment device during a transaction.

Guidelines

- For payment transactions requiring PIN entry into a personal cardholder device:
  - The transaction should be authorized online.
  - PIN verification should be performed offline by a secure cardholder token, for example, an integrated circuit (IC) card.
- For non-payment applications requiring PIN entry into a personal cardholder device one or both of the following should be applied:
  - Only offline PIN verification should be performed.
  - The device should not be capable of magnetic stripe transactions.
- Personal cardholder devices for PIN entry should be one of the following:
  - Issued to cardholders by the issuer or its approved agents. Issuers should warn cardholders not to purchase, use or acquire additional devices from a source other than their issuer.
  - A cardholder's personal device permitted by the issuer for the intended use.
- Personal cardholder devices for PIN entry should be one or more of the following:
  - Functionally secure i.e. compromisable only by physical means and the functionality cannot be subverted by unauthorized input into the device.
  - Providing a level of logical security to protect the PIN and other account assets.

- Processing insufficient individual cardholder data items to create cardholder payment device clones.
- Issuers are responsible for educating the users of permitted personal cardholder devices for PIN entry as to the precise cardholder's responsibilities for device management and protection.
- Issuers should provide clear, unequivocal guidance to cardholders as to when PIN entry is required.
- Issuers should provide a means to cardholders using a personal cardholder device for PIN entry to enable the cardholder to verify that a communication is genuinely with the issuer. For example the personal cardholder device could be a CAP reader.
- If the personal cardholder device is connected online or offline (even for other applications) it should be possible for the cardholder to determine that a genuine end to end dialogue with the issuer is in place rather than with phishing or other MITM malware that may be masquerading as the application requiring PIN entry.
- If the personal cardholder device is used at an issuer location see Personal PIN entry devices provided at Issuer locations section.
- Issuers should provide for secure processing of the PIN on the cardholder payment device. For example use of a payment-system brand approved ICC.
- Devices should not process more information than that needed for a transaction.
- Issuers should provide secure transmission of the PIN from the cardholder payment device to the issuer.
- Issuers should check for the presence of a magnetic stripe during a magnetic stripe transaction, i.e. authorization should not rely solely on online PIN verification and correctness of the PAN.
- Card holder payment devices using a server based payment application which requires the PIN as a CVM should provide mutual authentication between the client on the device and the remote server accessed by the client.
- Installed applications should have default settings set for security, rather than expect the cardholder to configure them.
- Issuers should provide secure provisioning of PIN processing software when personalized to a cardholder payment device post issuance.
- Issuers should provide for remote blocking of personalized applications.
- Issuer should provide cardholders with easy access to applicable malware countermeasures for the device used for PIN entry.

- PC based Issuer PIN management applications should provide a mechanism to protect a PIN during a transaction in case of 'Man in the Browser' or other rootkit attacks that may not be detected by common antivirus countermeasures. For example an offline personal authentication device (e.g. a CAP reader) used with an ICC can be used to sign payee account details and payment information during a transaction.
- Passcodes used to enable PIN CVM functionality should be different from the PIN.

Personal PIN Entry Devices Provided at Issuer Locations

Personal PIN entry devices provided by the issuer for use at an issuer location should be subject to rigorous device management. The inventory of devices should be checked daily. Each device should have a unique identifier within the inventory.

PIN Generation

Objective

PIN generation, whether performed by the cardholder or the card issuer, should be done in such a way that no individual other than the cardholder has the means to determine whether any PIN is any more likely to be correct than any other PIN. The number of possible PINs should be large enough to ensure that the probability of guessing the correct PIN given the number of attempts possible is sufficiently small. PINs should contain at least four numeric digits as per payment-system brand standards.

The entry of a reference PIN into a chip card or the loading of PIN-related data onto a magnetic stripe card at an approved issuer location, should be performed in such a way that the PIN value cannot be derived by unauthorized means..

The entry of a 'changed reference PIN' into a chip card should be performed in such a way that no individual other than the cardholder can make the change.

Threats

- Insiders or hackers gain unauthorized access :
  - to card and PIN production data at production site.
  - to transmitted production data between participating vendors and /or issuer systems.
  - Unauthorized access to PIN mailers and associated cards.
- Cryptographic algorithms used to generate PINs and / or associated verification parameters are compromised.
- See also PIN related Key management, PIN handling device management , PIN Transmission and PIN Storage sections.

General Guidelines

- Issuers should provide one or more of the following three options for PIN generation:
  - Issuer assigned derived PIN, generated using an appropriate cryptographic algorithm with an appropriate key length commensurate with existing standards (for example ISO TR 14742).
  - Issuer assigned random PIN, generated using a Random Number Generator compliant with ISO/IEC 18031 and tested using NIST SP 800-22.
  - Cardholder Selected PINs using guidance such as that provided in ISO 9564.

See PIN related Key management section for information relating to management of PIN generation keys within a hardware security module (HSM)

See PIN handling device management for information relating to management of HSMs.

Offline PIN Generation

- The issuer should generate a reference PIN for an IC card if offline PIN verification is supported as a CVM. The stored reference PIN within the IC is identical to the transaction PIN entered by the cardholder.
- All PIN data (offline and online) should be protected from the point it leaves the system that generated the PIN data to the point where it is stored on the card in accordance with payment-system brand vendor requirements for card personalization.

Issuer Assigned PIN

- Issuer assigned derived PINs should:
  - be derived cryptographically from either the PAN and/or some other value associated with the cardholder
  - Not be statistically biased (based upon a recognized standard for measuring statistical bias).
  - Not be stored by the issuer.
- Issuer derived random PINs should be created using a true or pseudo-random number generator (for example using a random number generator compliant with ISO/IEC 18031 and tested using NIST SP 800-22). Generated PIN values should be unpredictable and uniformly distributed within a permitted set of values.

Cardholder Selected PIN

- Banks should advise cardholders against using the PIN as a credential for remote banking or any other service and provide for an alternative input format for remote banking credentials, e.g. forbidding all-numeric passwords. (See also General PIN management guidelines section).
- If the cardholder selects the PIN:
  - the cardholder should be provided with appropriate guidance for PIN selection and usage. (See General PIN management guidelines section)
  - the PIN value should be protected from the point of PIN entry and beyond (See sections: Cardholder PIN selection by internet and Cardholder PIN selection by IVR)

Cardholder Selected PIN by mail

- If the cardholder selects the PIN by mail the PIN advice form should:
  - provide unambiguous instructions for completion of the form
  - use a cryptographically derived reference or control number (See section on control number) to link the selected PIN to the account
  - use a reference or control number that does not disclose the account number
  - Not contain any information which directly relates the PIN to the cardholder's account, name, or address once completed by the cardholder.

- Any cryptographic keys used to generate or protect reference numbers should be managed in accordance with the key management section.
- The process should not involve issuer personnel handling plaintext PIN values that can be linked to an identifiable cardholder or their account.
- Receipt of the PIN advice form should be by authorized issuer personnel.
- Residues of PIN mailers should be destroyed as part of operational procedure.

Cardholder PIN Selection by Internet

PIN selection by internet requires the cardholder to communicate credentials to the issuer's PIN notification system via an intermediate internet based PIN advice function.

- PIN selection by internet should protect the PIN using commensurate cryptographic protection as when PINs are transmitted during transaction processing, until it arrives at the cardholder's computer.
- PIN selection by internet should be accomplished by instructing the cardholder to enter pre-established credentials: for example a control number, a chosen PIN and authentication values.
- The control number and authentication values should not disclose the account number.
- Any cryptographic key used to generate a control number should not be used for any other purpose and should be managed in accordance with ISO 11568.
- The control number should be generated and conveyed to the cardholder in such a way, e.g. by using a PIN mailer, so that no one other than the cardholder can associate the control number with that cardholder without detection.
- The system should have no way of associating a control number or the authentication values with the associated cardholder's name, telephone number, address or account number.
- The PIN selection function should exchange only strings of numbers, (a control number and authentication values) with the issuer PIN notification system.
- The PIN selection system should re-associate the control number with a specific account number, validate the cardholder (or the transaction if there is no mechanism for pre-registration of the cardholder as in an anonymous gift card) using the authentication values and retrieve the cardholder PIN for that account number.
- The control number/PIN/authentication values string should not be logged and should be deleted immediately after use.

- The PIN selection system should be designed and operated under strictly enforced procedures such that no individual is able to associate any control number, PIN or authentication values with any specific account number.
- The PIN selection via the PC should not be associated with any cardholder account data.
- The security of the PIN selection implementation is based on the premise that no individual can associate a control number with a specific account.
- Internet PIN selection should be protected using a secure channel established between the client application on the user's PC and the server according to the principles of ISO/IEC 11770. The implementation should take into account MITB attacks.
- Payment-system brand requirements may apply to third parties outsourced to perform the service.
- An issuer should ensure that the association of cardholder authentication credentials with the control number does not weaken the principle that the control number cannot be used to determine a specific account.
- Cardholder authentication should not be performed by the internet server. It should be performed by the back end issuer host system and only after the control number is re-associated with the specific account.
- Cardholder authentication and generation of the reference PIN should be done in real time during the session, with the success or failure reported back to the cardholder.
- Web servers should be configured to disable client side caching of web pages that display PINs and associated data during the internet session.

Cardholder PIN selection by IVR

- PIN selection by IVR should be accomplished by instructing the cardholder to enter pre-agreed credentials: a control number, their chosen PIN and authentication values.
- The control number and authentication values should not disclose the account number.
- Any cryptographic key used to generate a control number should not be used for any other purpose and should be managed in accordance with ISO 11568.
- The control number should be generated and conveyed to the cardholder in such a way, e.g. by using a PIN mailer, that no one other than the cardholder can associate the control number with that cardholder without detection.
- The communication to the cardholder should also contain the control number and instructions.

- The cardholder should be instructed to dial the Issuer's IVR PIN selection function and follow the prompts to enter their control number, their chosen PIN and one or more authentication values.
- The PIN selection function should perform no other function than PIN selection within a single session.
- The session should be terminated after the PIN selection has been performed.
- The system should have no way of associating a control number or the authentication values with a specific cardholder's name, telephone number, address or account number.
- The IVR PIN selection function should pass strings of numbers, (a control number, a corresponding PIN and authentication values) to the PIN selection system.
- The IVR PIN Selection system should re-associate the control number with a specific account number, validate the cardholder using the authentication values and convert and store the cardholder entered PIN as the reference PIN for that account number. It may perform these functions in real time or later.
- The control number/PIN/authentication values string should not be logged and should be deleted immediately after use.
- The PIN selection system should be designed and operated under strictly enforced procedures such that no individual is able to associate any control number, PIN or authentication values with any specific account number.
- Separate HSMs should be used for this process, and HSMs should not be shared between processing production traffic and IVR traffic.
- Any involvement of a Customer Service Representative (CSR) should not request the customer's name or account number.
- An IVR system taking part in the PIN selection call should have no way of associating a PIN selection call to the calling telephone number.

  NOTE: The control number may be the reversibly enciphered account number. Some issuers provide a means to allow the cardholder to enter an enciphered PIN on the IVR.
- Cardholder PIN selection may be treated as equivalent to card activation.
- The security of cardholder selected PIN by IVR is based on the premise that no individual can associate a control number with a specific account.

  In this case it is not necessary for an issuer; in their environment; to encrypt the control number/PIN pair as they pass through the system. It is recommended to encrypt the PIN within the PIN management system once it becomes associated with an account.
- Payment-system brand requirements may apply to third parties outsourced to perform the service.

- An issuer should ensure that the association of cardholder authentication credentials with the control number does not weaken the principle that the control number cannot be used to determine a specific account.
- Cardholder authentication should not be performed by the IVR system. It should be performed by the back end issuer host system and only after the control number is re-associated with the specific account.
- Cardholder authentication and generation of the reference PIN are done in real time during the session, with the success or failure reported back to the cardholder.

PIN Verification Values

- PIN verification values derived from the PIN and PAN should be random or pseudo-random.
- PINs and PIN Verification Values should not be trivially derived from publicly available information.

General Guidelines

- Online PINs created after personalization should be verified by the issuer using a verification value stored in the issuer host system.
- PIN generation processes should address synchronisation of online and offline PIN.
- Multiple cards associated with the same cardholder account should have distinct PINs.
- Banks may co-issue cards together with external partners outside the banking industry. The partners should then be equally concerned about PIN protection and management. If two applications reside on the same physical card, they should either have distinct security systems with discrete PINs distributed and managed through separate channels, or the bank partner should take total responsibility for the security infrastructure hence offering banking security levels to its non-bank partner.

PIN Transmission

Objective

PINs and associated account data transmitted from one system to another should be protected against disclosure and protect PIN integrity against any party eavesdropping on, or manipulating, the communications link. PIN integrity refers to the integrity of the relationship between the PIN value and any associated information such as user account data or transaction information.

Threats

- Phone tap/wire tap. (GSM, VoIP, DTMF tones may be in the clear)
- Reliance on network encryption (which is not under the application's control and which may not be present or may use a compromised cryptographic technique).
- Attacks against the cryptographic algorithms used to encipher PIN codes and provide PIN integrity.

Guidelines

- PINs should be protected during transmission by one or more of the following:
  - Provision of physical protection
  - Encryption of the PIN value
  - Dissociation of the PIN from account data, with the use of an encrypted reference or control number to maintain PIN integrity.
- The PIN transmission protocols should be designed such that the introduction of fraudulent messages, or modification of valid messages, does not yield any useful information regarding a PIN.
- Enciphered transmission of PINs and associated data should provide PIN integrity
- If the PAN is available, PINs should be enciphered using "PIN blocks" according to one of the methods specified in ISO 9564.

  Use of ISO PIN block format 3 is recommended
- If the PAN is not available,
  - the encrypted reference or control number uniquely linked to the PAN by the issuer (for example to avoid transmission of the PAN) should be used to construct a PIN block . The construction should provide the same security properties as provided by ISO PIN blocks.
  - the method used for formatting a PIN block prior to encryption should not enable the PIN to be recovered from the resulting ciphertext (e.g. by using rainbow tables)

- Any cryptographic algorithm used for protecting transmitted PINs, either for purposes of secrecy or integrity, should have a level of security appropriate to the task. This should be assessed according to the relevant international and industry standards (See ISO 11568) and to the current industry best practice.
- Unenciphered PIN transmissions should not contain any information that can be directly connected with the cardholder or the account. For example the transmitted PIN should be linked to the PAN of the cardholder account by use of an encrypted reference or control number.. The control number should only be generated by the issuer.
- Unenciphered PIN transmission should provide PIN integrity, for example use of a secure PIN mailer for PIN advice by post.

PIN Storage

Objective

PINs and associated account data should be stored in the minimum number of locations required for reliable operation of the systems. If it is necessary to store PINs, they should be stored in such a way that no issuer staff or third party can derive secret information relating to them. A stored PIN can only be changed by the issuer or the cardholder if authorized by the issuer. It is not recommended to store PINs if reliable operations can be achieved without storage.

Threats

- Entities become more of a target from insiders or hackers when PINs are stored on systems.
- Insiders or hackers gain access to internal systems storing PINs and associated data.

Guidelines

- PINs, associated data and/or secret keys used to protect PINs stored with them should only be stored in locations where their integrity and confidentiality can be protected.
- The PIN should be stored within the issuer's systems using one of the following methods:
  - as an enciphered data object using an industry standard cryptographic algorithm and key strength
  - as an enciphered data object that is distinct from any other enciphered data object created with the same PIN value but a different PAN.
- PIN encryption algorithms for storage in issuer systems should be based on the ISO 9564 standard.
- Reference PIN databases should protect the integrity of reference PINs
- Reference PIN databases should provide confidentiality of reference PINs by storing enciphered PIN values.
- PIN encryption should incorporate the account number or other data such that the verification process would detect substitution of any value for another stored value
- All devices in issuer systems used to store cleartext PINs or cleartext PIN-related keys should be designed and managed such that PIN information cannot be determined by manipulating inputs to the device. For example, accessing the device to translate stored PINs to non-secure PIN block formats and outputting the values encrypted by a key to compare against a fraudster's previously built table of all possible PINs listed in the clear along with their corresponding cryptograms built using the same cryptographic key used to output the real PINs.
- All aspects of the logical and physical design of the technology used in the

issuers PIN storage processes, including key management implementation, and the personnel policies and procedures should be subject to regular review by the issuers' internal audit function.

- The issuer's procedures and policies for the personnel employed in PIN storage and processing operations should include pre-employment vetting of personnel.
- During storage processes all security relevant operations should be completed under dual control.
- During storage processes issuer personnel should not handle plaintext PIN values that can be referenced to an identifiable account.
- The PIN cannot be stored on the magnetic stripe of a card .
- When the reference PIN is stored in an ICC, it should be a payment-system brand approved ICC.

PIN Logging

Journalisation or logging of transactions containing PINs should be avoided but if necessary should satisfy the following:

- Ensure the PIN is not in the clear
- Ensure the PIN and / or PIN block is not retained for longer than necessary to complete the transaction
- Cardholder claims relating to PIN disclosure and / or fraud are recorded in such a manner as to identify the possible source of failure or misuse.

PIN Processing

Objective

Any device holding PINs or PIN-related account data should protect the security (confidentiality and integrity) of this information while it is being processed within the device, or being transferred from one part of the device to another

Threats

- Criminals gain access to the back end systems that perform PIN verification and access:
  - PINs and associated data during storage
  - PINs and associated data during transmission
  - PINs and associated data during processing
  - Sensitive HSM functionality that can be exploited to perform unauthorized PIN processing.

  See also PIN handling device management.

Guidelines

- PINS should be protected during processing by the following:
  - Provision of physical protection
  - Use of HSMs. Use of separate HSMs with limited command sets enabled for production authorization processing vs. issuer only operations can help protect issuers.
  - Encryption of the PIN value using appropriate algorithms and key lengths.
  - Separation of the PIN from account data, for example use of an encrypted reference or control number to link the PIN to the PAN.

  See also General PIN management guidelines.
- A device that processes PINs or PIN-related information that consists of more than one physical component should :
  - Protect exchange of data by physical or by cryptographic means.
  - Use components such that sending one or more fraudulent messages to a component shall not yield any useful information regarding a PIN.

PIN verification

- Online PIN verification is the responsibility of the issuer and should be performed by the issuer or a designated service provider.
- The online PIN verification process involving the PIN supplied by the cardholder and the reference PIN retained by the issuer should only be performed within a HSM.

See the PIN handling device management section for information relating to HSM management.

See the PIN related Key management section for information relating to the management of PIN verification keys.

- Issuers should block an account after 3 consecutive failed on-line PIN verifications, after which the cardholder should be required to contact the issuer or their agent.
- Issuers should investigate unusual levels of non consecutive on-line PIN verification failures against an account.

  See also General PIN management guidelines.

PIN Related Key Management

Objective

All keys used to protect PINs should be managed in accordance with industry best practices (see ISO 9564, ISO 11568 and PCI PIN Security requirements). This includes the selection of techniques that minimize the risk to PIN security in the event that one or more devices that handle PINs are physically compromised:

Threats

- Physical access to the key management system premises or logical access to the host system by an unauthorized person or persons.
- Circumvention of access controls by an authorized user.

Guidelines

- Issuer PIN Key management policy should be consistent with PCI PIN Security Requirements, ISO 9564 and ISO11568 for the corresponding key types and cryptographic applications to ensure that the security levels applied to issuer PIN security management are the same as security levels applied to acquirer PIN security management.
- All access to cryptographic material and related devices should be recorded,with date, name and reason for access.
- A key should be generated using processes that ensure that it is not possible to predict any key or subset of keys. Issuer related keys must be used for their sole intended purpose, PVKs should not be used as CVV keys etc. Additionally, issuer keys must not be shared among different issuers.
- Verification keys, such as those used for PIN and Card verification, should be segmented across card portfolios to minimize exposure where card re-issuance may become necessary, e.g., in the event of key compromise. Different keys should be used where the issuer issues cards under more than one payment brand and across BIN ranges within a given card portfolio.
- Key check values should:
  - Be calculated using the full key
  - Not exceed 6 hexadecimal characters
- A key should be distributed using one of the following:
  - Enciphered under a key encryption key of equal or greater strength
  - As two or more key components using techniques based on dual control and split knowledge.
- Cleartext key components should only exist in one of the following forms:
  - In the safekeeping of an issuer authorised custodian
  - In secure physical storage (for example a safe), accessible only by the authorised custodian and their designated backup.
  - As a transported cleartext component.
  - In a SCD.

- Transported clear text key components should be in pre-serialised, separate, tamper-evident, packaging or in a SCD.
- If a key loading device is used to transport key components:
  - The device (or the part of it which contains the key component) should be a SCD
  - The device should only be operated by issuer authorised personnel.
- Key loading procedures should ensure that:
  - All participating devices and connections are inspected for monitoring or tampering
  - key loading is performed using dual control
  - key components are only combined within a secure cryptographic device, e.g, a HSM
- Keys should be replaced in accordance with the existing issuer key management policy[3].
- Keys used in a production environment should not be the same as keys used in a non-production environment (for example testing or development).
- Keys should exist in the minimum number of locations needed for correct operation of the system in accordance with issuer security policy.
- Issuer security policy should identify suspicious circumstances that indicate a key compromise (consistent with their own fraud detection systems and threat analysis).
- In the event of a suspected key compromise:
  - The key and its derivatives should be replaced immediately
  - Replacement keys should not be derived from the compromised key
  - The compromised key, and its components should be destroyed
  - All keys protected by or derived from the compromised key should be destroyed
  - Users of compromised keys should be informed of the compromise and change in key, even if the key is no longer in use
  - The decommissioning of compromised keys should be logged
  - The amount of time in which a compromised key remains active should be consistent with the risk to affected parties
- PIN encryption keys should be used only for PIN encryption and not for any other purpose.
- Reference PINs should be protected using a different key to that used to protect transaction PINs, both for storage and transmission.
- Encryption keys should be unique to each pair of communicating nodes. .
- The strength of encryption mechanisms should be sufficient to minimise the risk of security breaches through exhaustive key search or through cryptanalysis.

[3] Key change intervals should be consistent with the corresponding PCI DSS requirements for key change intervals.

Key Management Using Internet Channels

- Transient working keys used for PIN encryption between a Web server and cardholder PC should be established across a secure channel according to the principles of ISO/IEC 11770 and deleted after the session.

PIN Handling Device Management

Objective

All devices that may contain PINs, or information that could be used to derive information about a PIN, should be designed to offer protection of the information stored within the device

These devices include ICCs used to process offline PINs, HSMs used to perform PIN processing and cryptographic devices used for cryptographic key management.

Threats

- ICC vulnerability increases with age. If a device has been issued and deployed for a long period of time (in excess of 5 years) an attacker may collect sufficient detailed design knowledge and/or attack techniques may evolve sufficient to compromise the device.
- Misuse of HSMs processing PINs. PINs can be revealed by using issuer functionality at an acquirer HSM or manipulating PIN block translation functionality between different formats.
- Misuse of HSMs processing PINs at a service provider site. PINs can be revealed at third party sites if they do not apply the physical and logical security requirements that are compatible with the issuer's security policy.

Guidelines

- Cryptographic devices should be kept up to date with current threat levels against cryptography via appropriate key management and software upgrades. Devices should be replaced when they can no longer provide adequate physical or cryptographic protection.
- Issuer HSM management policy should maintain parity with PCI PIN Security Requirements
- New issuance of ICCs should be based upon current payment-system approved devices (i.e. not a stockpile of devices with expired approvals).
- ICCs should be re-issued regularly (e.g. every three years).
- Software updates in all cryptographic devices should be cryptographically validated for integrity and as being from an authentic source, or supplied through verifiable procedures under dual control.
- HSMs used for PIN processing should meet PCI HSM Security requirements.
- All HSM command sets should be validated to ensure only the necessary commands are enabled and high risk command sets are disabled.
- Hardware and software used for PIN management should provide the following assurance:
  - It is performing its designed function and only that function,

  - The hardware and software cannot be modified or accessed without detection and / or disabling,
  - Information contained within the hardware or software cannot be fraudulently accessed or modified without detection and rejection of the attempt, and
  - Systems use is restricted in such a way that it cannot be misused or used to determine PINs by exhaustive trial and error.
- HSMs should be fully accounted for from time of manufacture until decommissioned.
- HSMs should be inspected for modification or tampering prior to commissioning.
- HSMs should be operated according to the specified issuer policy.
- HSMs should be protected from misuse by implementation of:
  - Dual controls for all key management activity
  - Dual controls for all sensitive issuance activity e.g. PIN change against a fixed PAN or PAN change against a fixed PIN, that could be used to mount attacks on PINs
  - Physical controls to prevent unauthorized device tampering or bugging.
- HSMs used for PIN Issuance should be kept physically and logically separate from HSMs used for PIN transaction processing.
- HSMs used to store cleartext PINs or cleartext PIN-related keys for any length of time should be handled securely when taken out of service for any reason. All keys that have an impact on the HSM's security envelope should be deleted from the HSM.
- All HSM use should be fully accountable. The mechanism used to monitor HSM use should be incapable of modification without detection.
- When decommissioned, either the internal memory should be mechanically or electronically erased or the device should be physically destroyed.
- Production networks used to access HSMs should provide layers of authentication to prevent remote access to unauthorised HSM functionality, e.g. segmentation of networks containing HSMs and using layered protection techniques such as defense in depth.
- The production environment network security policy should be consistent with the security policy of HSMs accessed over the network.

Cardholder Authentication to PIN Management Systems

Issuers that allow cardholders to remotely manage their PINs via the internet or IVR may authenticate cardholders by providing credentials to a PIN management system. Vulnerabilities in these systems could lead to PIN compromise.

Objective

Cardholder access to PIN management functionality that enables a PIN to be revealed or changed should use a high assurance authentication mechanism. The implementation should ensure that this can be done in a way that minimizes the risk of exposure of the PIN and associated account data.

Threats

- If the credentials for accessing the PIN management system are the same as those displayed on the cardholder payment device, an attacker with access to the device could impersonate a cardholder to access the system.
- The channel used to access the PIN management systems may be compromised.
  - For example malware installed on a PC or installed to a mobile (root kits, sniffers and keystroke loggers, MITB, MITM) may retrieve cardholder data. Credentials can be recorded and transmitted to fraudsters.
  - DNS poisoning may lead to pharming attacks where the cardholder browser is redirected to a fraudulent website.
- Displayed cardholder data may be surfed or screen scraped.
- Vishing or SMSishing may be used to socially engineer the cardholder into entering credentials into a malicious application.
- Calling line identification can be spoofed.
- Calls to a nominated mobile number can be maliciously forwarded to another number without the cardholder's knowledge.
- A fraudster may impersonate the customer at an issuer branch and present forged documents to inexperienced issuer personnel.
- If unsolicited PIN management requests from the issuer to cardholders are possible, for example via call-center, email or SMS, a cardholder may be socially engineered into revealing login credentials.

Guidelines

- Cardholders should be provided with a means to determine that a dialogue with the issuer is genuine.
- Cardholder authentication credentials should not be based on information that is publicly available.
- Cardholder authentication credentials should not enable a specific cardholder account to be determined from them.

- It should not be possible to authenticate a cardholder to the PIN management system solely using information obtained from the cardholder payment device. Card information may be used to confirm cardholder identity.
- Credentials for cardholder authentication to PIN management functionality should vary each time the cardholder accesses the system.
- Issuers should not transmit PAN or other account data to the cardholder during PIN management transactions.
- Issuers should avoid use of the transaction PIN as a credential for non-payment transactions, including e-banking access or access to the PIN management system.
- PIN management requests should be acknowledged back to the Cardholder by the issuer.
- The Issuer should avoid sending unsolicited PIN management requests and advise the Cardholder that this is the case.
- Cardholders should be provided with a means to audit the outcome of a PIN management request.
- Calling-line identification (CLI) should not be used as a sole means of cardholder authentication.
- CLI is vulnerable to caller-id spoofing. It may be used as a confirmation of a cardholder's identity but not a proof.
- Cardholder PIN management functions that require transmission of the PIN over open networks should provide assurance to the issuer and the cardholder that the correct PIN is only being delivered to or from the genuine cardholder. For example a separate communication channel could be used to deliver an acknowledgement.
- If the cardholder is contacted via telephone using a pre-registered number, the individual answering the phone should not be assumed to be the cardholder.

Use of Displayed Card Data

- The full PAN should not be used as an authentication credential for PIN management.
- The displayed card verification code may be used to verify the presence of the cardholder
- The displayed expiry date may be used to verify the presence of the cardholder

PIN Advice

Objective

Plaintext PINs and associated account details should only be visible to cardholders.

Threats

- A cardholder doesn't destroy the mailer or message containing the PIN.
- A cardholder family member gains access to the cardholder payment device and PIN after delivery.
- An insider at a mail sorting office intercepts the PIN mailer and the cardholder payment device.
- An insider at a mail sorting office intercepts the PIN mailer and the cardholder payment device, creates cloning data, then forwards both to the cardholder- possibly avoiding detection.
- A telephone engineer eavesdrops call traffic to a call center or IVR.
- IMSI grabbers eavesdrop GSM communication.
- Internet Service Provider personnel eavesdrop email and internet traffic.
- IVR or web systems may be subject to hacking or eavesdropping. Retrieved PIN and cardholder data may be sufficient to clone a cardholder payment device.
- Issuer PIN storage systems used for PIN delivery may be hacked.
- Cardholder PCs or mobile phones used for PIN advice may contain malware that can forward PIN and cardholder data to criminals.
- A fraudster impersonates customers and socially engineers a bank representative to change cardholder addresses so that cards and PINs are redirected.

Guidelines

- Card issuer personnel should only handle plaintext PINs when the associated account details are not available to them.
- A PIN should only be distributed to a pre-registered cardholder destination. The destination address will depend upon the delivery method.
- The issuer should validate a change of destination request from the cardholder.
- Issuers should periodically re-examine their procedures for delivering cards and PINs to cardholders.

PIN advice by mail

- The PIN mailer should not reveal the plaintext PIN until it is opened.
- PIN mailer stationery should be treated as a form of secure device, and issuers should ensure that the PIN is not obtainable without tampering being evident.
- The envelope should display the minimum data necessary for delivery to the correct cardholder.
- A card and PIN:
  - should:
    - be sent at least 24 hours apart
  - should not:
    - be transmitted in the same package
    - be sent on the same day.
    - not be sent on the last working day before the weekend or a holiday.
- Cards should not be mailed in large batches. Mixing envelopes containing cards with other general mail increases the effort of stealing a large number of cards from the mail system at one time.
- Cards should be mailed 'inactivated' and should require activation by the cardholder.
- Card issuance should support last minute cancellation (e.g., removing cards from mailing queue) when an applicant or customer is deemed "high risk."
- Use express delivery when mailing cards to high risk areas or foreign countries.

PIN advice by voice

- Card issuers should not permit spoken communication of the plain text PIN by a human operator.

PIN advice in person at Issuer Location

- Card issuers should not permit spoken communication of the plain text PIN by a human operator.
- Authorized Issuer personnel should obtain and verify identification of the cardholder as required by the issuer policy.
- The issuer's PIN management system should authenticate the issuer personnel used to perform PIN advice.
- The authorized employee should initiate the PIN advice process.
- The process should terminate upon completion of the PIN advice.
- A transaction log should provide the authorized employee's identification together with the date and time.

PIN Advice by SMS

- The issuer should provide the cardholder with security guidance for the management of mobile phone used for PIN advice. This should advise the cardholder about the risks of mobile malware and of storing account data on the mobile phone.
- The mobile number to be used for SMS PIN advice should be pre-registered with the issuer.
- A cardholder request to transmit a PIN via SMS to a mobile number which has not been pre-registered with the issuer should require re-authentication of the cardholder according to issuer policy.
- The SMS advice should be preceded by a communication to the cardholder containing an identification value or control number and an authentication value.
- The identification value or control number and authentication value should be communicated to the cardholder by a different mechanism than SMS
- The identification value and authentication values should not disclose the account number.
- If the identification value used by the issuer is a publicly available data item such as the cardholder's telephone number or email address then a second non-public authentication mechanism or value should be used. This authentication value or mechanism can be selected by the issuer.
- The PIN distribution system should run on a dedicated computer and be isolated from any other network by a dedicated firewall.
- All PINs, control values and authentication data should be encrypted using Triple DES or AES with a minimum key length of 112 bits during transmission to and storage in the PIN distribution system.
- Issuers should use a 'pull' mechanism for SMS PIN advice.
- The cardholder should be instructed to contact the PIN distribution system to request their PIN e.g. sending an email or SMS or dialing an IVR PIN distribution system.
- The PIN distribution system should identify the cardholder from the identification value supplied in the request for the SMS PIN advice. The request should also contain the cardholder's authentication value.
- The PIN distribution system should perform no other function than PIN distribution and any sessions established during the distribution (e.g. a telephone call) should be terminated once the PIN has been sent.
- The distribution system should have no way of associating an identification value or authentication value with a specific cardholder's name, address or account number.
- The PIN distribution system should only send the PIN to the cardholder on successful validation of the authentication value.

- The PIN distribution system should have a fail-safe feature that limits the number of attempts made to obtain a PIN. This system feature should alert the service provider whenever this parameter is exceeded.
- When the PIN is to be sent to the cardholder, it may be decrypted and a string of numbers passed to the distribution mechanism or channel (e.g. the PSTN operator or email system).
- The PIN distribution system should not contain any other cardholder data (e.g. PAN, cardholder name).
- The association of the PIN to a specific account should not be possible with the authorised information available in the distribution system.
- The PIN distribution system should not link to any other system where associated cardholder data could be accessed.
- The identification value, PIN and authentication value should not be logged and should be deleted immediately after successful delivery is confirmed.
- If the PIN is not delivered to the cardholder then it should be deleted from the system after the period required by issuer policy.
- It should not be possible to identify the type of cardholder payment device or the account from the SMS message containing the PIN.

PIN Advice by Internet

PIN advice by internet requires the cardholder to communicate credentials in exchange for the PIN to the issuer's PIN notification system via an intermediate internet based PIN advice function.

- The issuer should provide the cardholder with security guidance for the management of PCs used for PIN management . This should include advice about the risks of malware and of storing account data on the PC.
- PIN advice by internet should protect the PIN using commensurate cryptographic protection as when PINs are transmitted during transaction processing, until it arrives at the cardholder's computer.
- PIN advice by internet should be accomplished by instructing the cardholder to enter pre-established credentials: for example a control number, a chosen PIN and authentication values.
- The security of the PIN advice implementation is based on the premise that no individual can associate the control number with a specific account.
- The control number and authentication values should not disclose the account number.
- The control number and authentication values should be communicated to the cardholder using a different mechanism
- Any cryptographic key used to generate a control number should not be used for any other purpose and should be managed in accordance with ISO 11568.

- The control number should be generated and conveyed to the cardholder in such a way, e.g. by using a PIN mailer, so that no one other than the cardholder can associate the control number with that cardholder without detection.
- The control number should be communicated to the cardholder in such a way that no one other than the cardholder can have access to it without detection. The system should have no way of associating a control number or the authentication values with a specific cardholder's name, telephone number, address or account number.
- The PIN advice function should exchange only strings of numbers, (a control number and authentication values) with the issuer PIN notification system.
- The PIN notification system should re-associate the control number with a specific account number, validate the cardholder (or the transaction if there is no mechanism for pre-registration of the cardholder as in an anonymous gift card) using the authentication values and retrieve the cardholder PIN for that account number.
- The control number/PIN/authentication values string should not be logged and should be deleted immediately after use.
- The PIN advice system should be designed and operated under strictly enforced procedures such that no individual is able to associate any control number, PIN or authentication values with any specific account number.
- The PIN delivery to the PC should not be associated with any cardholder account data.
- Cardholder PIN advice may be treated as equivalent to card activation.
- Internet PIN advice should be protected using a secure channel established between the client application on the user's PC and the server according to the principles of ISO/IEC 11770. In addition the implementation should take into account MITB and other malware attacks.
- Payment-system brand requirements may apply to third parties outsourced to perform the service.
- An issuer should ensure that the association of cardholder authentication credentials with the control number does not weaken the principle that the control number cannot be used to determine a specific account.
- Cardholder authentication should not be performed by the internet server. It should be performed by the back end issuer host system and only after the control number is re-associated with the specific account.
- Web servers should be configured to disable client side caching of web pages that display PIN and associated data during the internet session.

PIN Advice by IVR

PIN advice by IVR requires the cardholder to communicate credentials in exchange for the PIN to the issuer's PIN notification system via an intermediate IVR PIN advice function.

- PIN Advice by IVR should be accomplished by instructing the cardholder to enter pre-agreed credentials: a control number and authentication values.
- The control number and authentication values should be communicated to the cardholder using a different mechanism.
- The control number and authentication values should not disclose the account number.
- Any cryptographic key used to generate a control number should not be used for any other purpose and should be managed in accordance with ISO 11568.
- The control number should be generated and conveyed to the cardholder in such a way, e.g. by using a PIN mailer, that no one other than the cardholder can associate the control number with that cardholder without detection.
- The communication to the cardholder should contain the control number and instructions.
- The cardholder should be instructed to dial the issuer's IVR PIN advice function and follow the prompts to enter their control number and one or more authentication values.
- The IVR PIN advice function should perform no other function than PIN advice within a single session.
- The call should be terminated after the PIN advice has been performed.
- The IVR system should have no way of associating a control number or the authentication values with a specific cardholder's name, telephone number, address or account number.
- The IVR PIN advice function should exchange only strings of numbers, (a control number and authentication values) with the issuer PIN advice system.
- The PIN notification system should re-associate the control number with a specific account number, validate the cardholder (or the transaction if there is no mechanism for pre-registration of the cardholder as in an anonymous gift card) using the authentication values and retrieve the cardholder PIN for that account number.
- The control number/PIN/authentication values string should not be logged and should be deleted immediately after use.
- The PIN advice system should be designed and operated under strictly enforced procedures such that no individual is able to associate any control number, PIN or authentication values with any specific account number.

- Any involvement of a Customer Service Representative (CSR) should respect the principles of PIN advice by IVR and should not request the cardholder's name or account number.
- The IVR system taking part in the PIN advice call should have no way of associating a PIN advice call to the calling telephone number.
- Cardholder PIN advice may be treated as equivalent to card activation.
- The security of PIN advice by IVR is based on the premise that no individual can associate a control number with a specific account.
- Payment-system brand requirements may apply to third parties outsourced to perform the service.
- An issuer should ensure that the association of cardholder authentication credential with the control number does not weaken the principle that the control number cannot be used to determine a specific account.
- Cardholder authentication should not be performed by the IVR system. It should be performed by a separate back end issuer host system and only after the control number is re-associated with the specific account.

Call Center Use

- Issuers should ensure that call-center services are unable to divert PIN or sensitive cardholder information to an unauthorized destination for later retrieval.
- Where possible, call center personnel activity should be analyzed against compromised cardholder accounts processed by the personnel.
- Call center personnel should not request a cardholder to divulge their PIN in an oral or written manner.

Generation of the Control/ Reference Number Linked to the PAN

- Any cryptographic key used to generate the control number should not be used for any other purpose.
- Any cryptographic keys to generate the control number should be managed in accordance with the PIN related Key management section.

PIN Change

Objective

Plaintext PIN values and associated account details should only be visible to the associated cardholders.

Threats

- Customer may select a PIN value that is easy to guess.
- See also PIN Advice threats

Guidelines

- Cardholder PIN change can be performed using any issuer approved device and functionality.
- PIN change should follow principles of ISO-9564.
- PIN change should not be performed by email
- PIN change should not be performed using an intermediate human interface to update the PIN
- PIN change events should be recorded for future dispute resolution.
- PIN change event logs should not include any plaintext PIN values. (See PIN Logging section)
- A PIN change should be handled differently from a forgotten PIN.

  Proof that the current PIN is known is an indicator that the request to change the PIN is from the genuine cardholder.

PIN change at Issuer Location

- At a card issuer's location, on-line PIN change should be supported through an ATM, or a secure unattended device.

  See Cryptographic Device management for guidance on providing a secure unattended device.
- The procedure should require the current PIN to be entered and verified before selection and activation of the new PIN otherwise the cardholder should be directed to the 'forgotten PIN' procedure.
- The new PIN should be entered twice and the terminal should confirm that the two entries are identical.
- The terminal should have a user interface that is easy for a cardholder to use, for example clearly displayed, unambiguous instructions.
- The terminal should be functionally secure so that:
  - displayed messages cannot be modified in an unauthorized way (For example "Enter PIN" message cannot be displayed when data is output in clear).

  - The keyboard is controlled by secure logic.
- The terminal should be designed to ensure that PIN management data, cannot be accessed by an application that has been loaded in an unauthorised way.
- The terminal should provide a "clear" key to correct single digit errors during PIN entry.
- The terminal should be equipped with a privacy shield.
- If CCTV is used within the issuer location it should not be able to observe PIN entry.
- The terminal and the operational environment should provide protection against exhaustive PIN searches, e.g. by the terminal blocking itself or being blocked after a suspiciously high proportion of incorrect PINs attempts.

PIN change by mail

- Cardholder PIN change by mail should use the same process as cardholder selected PIN by mail.

IVR PIN change

- See section on IVR PIN advice.

PIN change using the internet

- See section on PIN advice using the internet

Offline PIN change

- The PIN change protocol should support synchronisation of the off-line and on-line PIN (when an on-line PIN exists) by recognizing exception conditions such as time-outs.
- Unless the protocol demonstrates that both the on-line and the off-line PINs have been changed successfully, the offline PIN value should roll back (where possible) to the original PIN value.
- Transaction protocols at ATMs should ensure that the on-line and off-line PINs are always aligned. Thus, any failures, such as "time-outs" will result in a "roll-back" to the original PIN .
- If an on-line PIN update has been completed, but the off-line PIN update has not been completed for any reason there is the risk that the on-line and off-line PIN values are not synchronised. Issuers should implement procedures to identify such a condition when it occurs and to display appropriate instructions to the cardholder.

Additional PIN Management Functions

Threats

- Infrequently used PIN management procedures and exceptions can be exploited if the procedures and policies applied to them are unfamiliar to issuer personnel or are implemented less securely than the standard PIN management procedures. For example a lower assurance authentication mechanism may be used to identify the cardholder

Special Procedures for PIN Management

- Where any special procedures are used to manage PINs, for example to blind or partially sighted cardholders, these procedures should be carefully vetted and rigorously applied to avoid a greater possibility of compromise. For example a P2P contact may be required.

Compromised PIN

- Issuers should specify the suspicious events that indicate a PIN is suspected of compromise.
- If a PIN is suspected of compromise
  - The compromised PIN should be deactivated as soon as possible,
  - The cardholder should be informed of options available to request a new PIN,
  - The replacement PIN should not intentionally be the same as the compromised PIN
  - Activation of the replacement PIN may be implicit or explicit
  - If the compromised PIN was a derived PIN, then at least one element used in deriving the prior PIN should be changed when the new PIN is created.
  - Fraudulent transactions must be reported to the networks in accordance with payment-system brand rules

Forgotten PIN

- If a cardholder forgets his/her PIN:
  - The new PIN should not be replaced within an interchange environment,
  - The PIN replacement should be performed through the issuer's systems

PIN UNBLOCK

- Card issuers may choose to implement additional or alternative security measures before executing the PIN UNBLOCK function through an ATM, in which case the ATM display should advise cardholders to contact the card issuer.
- Chip enabled ATMs should support Issuer Script Messaging and the PIN CHANGE/UNBLOCK command.
- Cardholders should be provided with unambiguous guidance for the PIN UNBLOCK procedure.

- Cardholders should be informed at the ATM whether PIN UNBLOCK has been successfully applied.
- When a PIN-blocked card has successfully completed an on-line PIN verification at an ATM, the issuer should unblock the PIN.

PIN Activation

- A PIN may be activated either implicitly or explicitly. If the PIN activation is explicit:
  - Receipt of the PIN by the cardholder should be acknowledged through signed and verified means.
  - Neither the PIN Receipt nor the response should contain the PIN.

PIN Deactivation

- The PIN should be deactivated by the issuer when one or more of the following occur:
  - The PIN is or is suspected to be compromised,
  - All accounts associated with the PIN are closed,
  - The issuer determines that deactivation is appropriate,
- In the case of a PIN compromise, or a deactivation request by the cardholder, the cardholder should be advised of the action taken,
- The issuer should take appropriate measures to ensure the deactivated PIN cannot subsequently be used with its original associated accounts.