SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Card Present PIN

INTRODUCTION TO THE PAYMENT LIFECYCLES AND SECURITY PROFILES

Consumers and organizations have a variety of options for making and receiving payments. While these payment types share the ultimate goal of transferring funds from payer to payee, the path those funds travel and the approaches employed for safely and securely completing transactions vary. The Secure Payments Task Force developed the Payment Lifecycles and Security Profiles as an educational resource and to provide perspectives related to:

- The lifecycles of the most common payment types, covering enrollment, transaction flow and reconciliation
- Security methods, identity management controls and sensitive data occurring at each step in the payment lifecycles
- Relevant laws and regulations, and other references, as well as challenges and improvement opportunities related to each payment type

The profiles employ a consistent format for describing the lifecycle of each payment type. The lifecycle template is not designed to represent the nuances of specific payment transaction flows, but as a broad taxonomy that can be applied across different payment types for understanding and comparing controls and risks. The profiles are not all-encompassing in describing the layered security strategies that may be employed by specific networks, providers or businesses and shouldn't be considered an assessment of overall security of different payment types. The improvement opportunities noted in the profiles highlight areas for further industry exploration and are not intended as guidance or specific solutions to be implemented.

These valuable resources were developed through the collaborative efforts of more than 200 task force participants with diverse payments and security expertise and perspectives. It is the hope of the task force that by helping industry stakeholders better understand these payments processes, the security and risks associated with these processes, and potential improvement opportunities, they will be well positioned to take action to strengthen their payment security practices.

The Card Present PIN Payment Lifecycle and Security Profile maps out the lifecycle of a Card Present PIN payment to establish a common understanding of the payment journey and serve as an educational reference guide for payments and security stakeholders.

Payment Lifecycle and Security Profile information includes:

1) Payment Flow Overview;
2) Payment Type Operation;
3) Overview of Security Methods and Associated Risks;
4) Inventory of Sensitive Payment Data and Associated Risks;
5) Overview of Laws, Regulations, and References on Payment Security (including Challenges and Improvement Opportunities).

CARD PRESENT PIN

Definition: A payment card (e.g. credit or debit) transaction whereby the cardholder presents the card and enters a personal identification number (PIN), a secret numeric password known only to the cardholder and a system, to authenticate the cardholder to the system, and/or biometric authentication which authenticates the cardholder to the device and would include attributes used by the issuer for risk evaluation. The cardholder is only granted access if the PIN provided matches the PIN in the system and/or biometric authentication of the device. PINs are used throughout the industry and include ATM, Point of Sale (POS), Mobile Wallets, and E-commerce transactions. A PIN may also be used to complete a debit card transaction where the magnetic stripe of the card is swiped at the point of sale or transactions, an EMV Chip card transaction where the chip of the card is inserted at the point of sale and the PIN replaces the cardholder's signature to authorize the transaction, or on E-commerce sites where a virtual PIN pad is enabled.

Note: These materials have been created by the Secure Payments Task Force and are intended to be used as educational resources. The information provided in the Payment Lifecycles and Security Profiles does not necessarily reflect the views of any particular individual or organization participating in the Secure Payments Task Force. The document is not intended to provide business or legal advice and is not regulatory guidance. Readers should consult with their own business and legal advisors.

PAYMENT FLOW OVERVIEW AND PAYMENT TYPE OPERATION

			GENERIC FUNCTIONAL STEP	CREDIT OPERATION	DEBIT OPERATION
ENROLLMENT			**Payer ID / Enrollment** Enrollment of a payer includes identity (ID) proofing, management of users (enrollment, de-enrollment and changes) and determination of authority based on role	Individual or organization requests credit account with issuer. Issuer verifies customer information in accordance with their Know Your Customer (KYC) program. PIN can be created by consumer or uniquely randomly generated by financial institution. The PIN associated with the account may be communicated to the cardholder via direct outreach, email, or physical mail.	Individual or organization requests credit account with issuer. Issuer verifies customer information in accordance with their Know Your Customer (KYC) program. PIN can be created by consumer or uniquely randomly generated by financial institution. The PIN associated with the account may be communicated to the cardholder via direct outreach, email, or physical mail.
			Payee ID / Enrollment Enrollment of a payee includes identity (ID) proofing, management of users (enrollment, de-enrollment and changes) and determination of authority based on role	Acquirer approves merchant Merchant is registered in advance and identification data is attributed when registered by the acquirer.	Acquirer approves merchant Merchant is registered in advance and ID data attributed when registered by the acquirer
TRANSACTION	Payer Authentication	PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS	**Payer Authentication** Verification of payer when originating payments	Cardholder and card verification methods include PIN and Primary Account Number (PAN) along with other items such as expiration date, Card Verification Values[1], EMV Application Cryptogram.	Cardholder and card verification methods include PIN and Primary Account Number (PAN) along with other items such as expiration date, Card Verification Values[1] , EMV Application Cryptogram.
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Point of sale (POS), ATM, mobile, internet, other omni channel solutions	Point Of Sale (POS), ATM, mobile, internet, other omni channel solutions
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	Secure cryptographic device (SCD) which meets physical and logical security standards. Examples include ATM, PIN Entry Device (PED) terminal, mobile	Secure cryptographic device (SCD) which meets physical and logical security standards. Examples include ATM, PIN Entry Device (PED) terminal, mobile
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Credit account	Demand Deposit Account (“DDA”)
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	Merchant, acquirer, association or network, processor, issuer	Merchant, acquirer, association or network, processor, issuer
	Payer Authorization		**Payment Network Traversed** “Rails” used to route authorization requests to the holder of the funding account	Authorization occurs through payment networks (e.g. credit networks).	Authorization occurs through payment networks (e.g. debit networks).
			Transaction Authorization Determination of whether to approve or decline a transaction including authorization time-frame, obligations, and any recourse decisions	Transactions are approved or declined by the issuer within payment network service level agreements (SLAs).	Transactions are approved or declined by the issuer within payment network service-level agreements (SLAs).
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	Payment network or acquirer rules dictate format exchange rules.	Payment network or acquirer rules dictate format exchange rules.
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use	Transaction approval is confirmed at device used to initiate transaction.	Transaction approval is confirmed at device used to initiate transaction.
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)	Acquirer authenticates merchant to accept files and get paid.	Acquirer authenticates merchant to accept files and get paid.
	Clearing and Settlement		**Settlement / Exchange of Funds** Actual movement of funds to settle funding arrangements and applicable fees	Settlement occurs per payment network rules (e.g. credit networks).	Settlement occurs per payment network rules (e.g. debit networks).
RECONCILIATION			**Reconciliation / Exception Handling** Process and responsibilities associated with reconciling and handling any exceptions or problems with a payment	Disputes are required to be reported/ processed within specified timeframe defined by payment network or card rules and law.	Disputes are required to be reported/ processed within specified timeframe defined by payment network or card rules and law.
			User Protection / Recourse Applicable rules, regulations, and legal means of recourse	Determined by payment network rules and applicable consumer protection laws and regulations. Regulation Z’s consumer protections apply to consumer credit.	Determined by payment network rules and applicable consumer protection laws and regulations. Regulation E’s consumer protections apply to consumer debit.

OVERVIEW OF SECURITY METHODS AND ASSOCIATED RISKS

		SECURITY METHODS	RISKS
ENROLLMENT	PAYER ID / ENROLLMENT	Issuer verifies the individual during enrollment before issuing a card. Know Your Customer (KYC), Customer Identification Program (CIP), background checks, etc.; ID verification of a 'carbon-based life form' Employee training Issuers may utilize anomaly and fraud detection tools to help identify suspicious or fraudulent activity associated with a specific account or group of accounts.	Social engineering (e.g. call center or end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Account takeover Synthetic Identity: Use of stolen identity information combined with fraudulent information to create a new 'synthetic' identity which is used to open fraudulent accounts and make fraudulent purchases. Strong enrollment processes may help mitigate synthetic identity risk throughout the transaction process. Credential stuffing (e.g. automated injection of breached username/password pairs in order to fraudulently gain access to user accounts) Knowledge-based questions can be compromised.
	PAYEE ID / ENROLLMENT	Acquirer (or the agent of the acquirer) verifies the individual(s) or organizations enrolling as a merchant before establishing a merchant ID (KYC, CIP, background checks, etc.). Employee training	An individual could create a fake merchant account. Synthetic Identity: Use of stolen identity information combined with fraudulent information to create a new 'synthetic' identity which is used to open fraudulent accounts and make fraudulent purchases. Strong enrollment processes may help mitigate synthetic identity risk throughout the transaction process.
TRANSACTION		Chip, PIN, Hardware Security Module (HSM) all must be managed per X9 Standards and Payment Card Industry (PCI) PIN regulations. Encryption PIN blocks are well defined and are mostly universally standard. Hardware encryption systems utilize Triple DES encryption algorithm. Typical key management method is Derived Unique Key Per Transaction (DUKPT). Participants in the payment transaction (e.g. merchants, acquirers/processors, payment networks, and issuers) may utilize anomaly and fraud detection tools to help identify risks and mitigate fraudulent transactions. Anomaly and fraud detection tools may include transaction risk scoring, risk-based authentication, transaction history and real-time authorization/decline capabilities among others. Validate the integrity of the payment message. Review message format for inconsistencies. Employee training Consumer and corporate customer education Strong key management is also necessary using secure rooms and environments to store and load encryption keys into PIN Entry Devices (PEDs). Most POS systems transmit card data in the clear. Many organizations use data encryption solutions where the card data is encrypted from the point of sale to the acquirer. Physically secure devices which meet international security standards Tokenization may be used for card data storage and used for future returns or loyalty. As payments and technology continue to change, risk-based authentication is a way to continually evaluate and apply optimal security methods.	PIN verification is a form of multi-factor authentication. Skimming of card data and PIN's are a common form of attack. It is difficult for consumer to know if the merchant/ATM/POS is legitimate. Account takeover Social engineering (e.g. end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Machine takeover (e.g., payee, financial institutions, network/operator, payer) Transaction data may be altered or spoofed (e.g. counterfeit transactions, credit master attacks, brute force attacks, etc.). First party/theft/lost or stolen transactions Many organizations use data encryption solutions where the card data is encrypted from the point of swipe to the acquirer. Only the issuer can authenticate the PIN. There are methods of duplicating EMV Chip transactions where the encryption fails but some issuers were accepting them anyway. Sole reliance on a point in time compliance statement (minimal, "check the box" compliance) does not equal security. Some POS systems/applications transmit and/or store card data in the clear. End-to-end encryption is not universally applied in POS systems/applications. Inadequately-controlled enrollment often poses additional risk at the time of transaction. The speed of payment processing and reconcilement may impact the ability to identify fraud in time to recover funds.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Participants in the original payment transaction may utilize anomaly and fraud detection tools to identify suspicious patterns of activity that may warrant further investigation or potential modifications to transaction anomaly and fraud detection tools.	
	USER PROTECTION / RECOURSE		

INVENTORY OF SENSITIVE PAYMENT DATA AND ASSOCIATED RISKS

		SENSITIVE PAYMENT DATA (DATA THAT NEEDS TO BE PROTECTED)	RISKS ASSOCIATED WITH THE SENSITIVE PAYMENT DATA
		Sensitive payment data must be protected wherever it is processed, stored or transmitted	
ENROLLMENT	PAYER ID / ENROLLMENT	<u>Sensitive data used to enroll or open an account:</u> Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Signature **Any data that is inputted by the user (e.g. email)*	If compromised, this data can be used to fraudulently set up an account at a financial institution and be used for other identity theft crimes.
	PAYEE ID / ENROLLMENT	<u>Sensitive data used to enroll or open a merchant account:</u> Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Signature | Business Name | Tax ID	If compromised, someone that is not a merchant could create a fake merchant account. This could also occur if the merchant account is not fully vetted/authenticated prior to setting up the merchant account.
TRANSACTION		**The following data is considered Sensitive Payment Data:** <u>Cardholder Data:</u> *Cardholder data must be protected wherever it is processed, stored or transmitted.* Primary Account Number (PAN) Cardholder Name Expiration Date Service Code Signature <u>Sensitive Authentication Data:</u> *Sensitive Authentication Data must be protected and must not be stored after authorization of the transaction.* Full Track Data (magnetic stripe data or equivalent on a Chip) Card Verification Values[1] PINs/PIN Blocks Encryption Keys PIN Offsets <u>EMV Data Elements:</u> Full Track Data equivalent on the Chip Application Authentication Cryptogram (AAC) Application Cryptogram Application Identifier (AID) Application Transaction Counter (ATC) Authorization Controls (aka Offline Risk Parameters) Authorization Request Cryptogram (ARQC) Card Authentication Method (CAM) Chip Card Security Code (iCVV, Chip CVC, iCSC) Dynamic Card Security Code (DCID, DCVC, DCVC3, DCVV)	Compromised cardholder data can be used by a criminal to create a fake credit/debit card for keyed, card present fraud (e.g. the magnetic stripe or Chip are not properly encoded and the merchant keys in the card number at the terminal) as well as card not present fraud at merchants that do not validate Card Verification Values[1] (or where the fraudster has already obtained the Card Verification Values[1]). Compromised sensitive authentication data can be used in conjunction with compromised cardholder data to create counterfeit credit/debit cards that can be used as if they were the actual cardholder.
	PAYEE AUTHENTICATION	<u>During transaction flow:</u> Merchant ID | Terminal ID | Terminal address | Merchant category code (MCC) | Terminal country code | Transaction currency code | Transaction type | Terminal entry capability | Merchant name	<u>During transaction flow:</u> If compromised, this data may be used to submit fraudulent payments into the payments system, especially for card testing purposes. If compromised, someone that is not a merchant could spoof a legitimate merchant.
	CLEARING AND SETTLEMENT	Issuing bank ABA number | Issuing bank settlement account number | Merchant bank ABA number | Merchant settlement account number	If compromised, this data may be used to make fraudulent debits to the settlement accounts.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Merchant ID <u>Cardholder Data*:</u> Primary Account Number (PAN) | Cardholder Name | Expiration Date | Signature **Cardholder data must be protected wherever it is processed, stored or transmitted*	If compromised, someone that is not a merchant could spoof a legitimate merchant. Compromised cardholder data can be used by a criminal to create a fake credit/debit card for keyed, card present fraud (e.g. the magnetic stripe or chip are not properly encoded and the merchant keys in the card number at the terminal), as well as card not present fraud at merchants that do not validate Card Verification Values[1] (or where the fraudster has already obtained the Card Verification Values[1])
	USER PROTECTION / RECOURSE		

[1] Card Verification Values: Card Verification Values represent data elements that are (1) encoded on the magnetic stripe or the Chip of a payment card; or (2) printed on the physical payment card and are used to validate the card information during the transaction authorization process. Card Verification Values encoded on the magnetic stripe (e.g. CAV, CVV, CVC, CSC) or on the Chip (e.g. dCVV, iCVV) are generated via a secure cryptographic process and may be static or dynamic data used to validate the card during the authorization process. Card Verification Values printed on the physical card (e.g. CID, CAV2, CVC2, CVV2) may be three-digit or four-digit codes printed on the front or back of the physical card that are uniquely associated with the physical card and ties the primary account number to the physical card. Note: Payment network rules and the Payment Card Industry (PCI) Security Standards Council provide additional definitions of Card Verification Values.

OVERVIEW OF LAWS, REGULATIONS AND REFERENCES ON PAYMENT SECURITY
(INCLUDING CHALLENGES AND IMPROVEMENT OPPORTUNITIES)

LEGAL AND REGULATORY REFERENCES

Debit cards (consumer) – Electronic Fund Transfer Act, 15 U.S.C. § 1693 *et seq.;* Regulation E. 12 CFR § 1005.2 *et seq.* (EFTA applies only to accounts "established primarily for personal, family, or household purposes" 15 U.S.C. § 1693a(2))

Credit cards (consumer) – Truth in Lending Act, 15 U.S.C. § 1601 *et seq.;* Regulation Z. 12 CFR § 1026.1 *et seq.* (TILA exempts "extensions of credit primarily for business, commercial, or agricultural purposes, or to governmental agencies or instrumentalities, or to organizations")

Prepaid cards (consumer) – Under CFPB Prepaid Accounts Rule (81 Fed. Reg. 83934 (November 22, 2016)) (to be codified at 12 CFR pts. 1005 and 1026), as amended on January 25, 2018, and effective April 1, 2019, Regulation E would apply to prepaid cards, with Regulation Z expanded to apply to prepaid cards with certain credit features.

Financial Crimes Enforcement Network (FinCEN) Bank Secrecy Act, 31 U.S.C. § 5311, *et seq.;* 31 CFR § 1010.100, *et seq.* (implementing regulations); FFIEC, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014).

Customer Identification Program (CIP), 31 CFR § 1020.220, *et seq.*

Identity Theft Red Flags Rules, 12 CFR § 41.90 (OCC); 12 CFR § 222.90 (FRB); 12 CFR § 334.90 (FDIC); 12 CFR § 717.90 (NUCA); 16 CFR § 681.1 (FTC); 17 CFR § 162.30 (CFTC); 17 CFR § 248.201 (SEC)

Board of Governors of the Federal Reserve System, Guidance on Managing Outsourcing Risk (Dec. 5, 2013) – FRB SR 13-19: Third party oversight guidance, set of cyber-risk oversight activities which includes reporting and expectations for Boards of Directors and Senior Management.

FFIEC IT Exam Handbooks: Some of the handbooks are more frequently a factor in exams, but they all contain provisions that impact payments compliance in the areas of confidentiality, availability, data integrity, privacy and third party oversight.

- FFIEC, IT Examination Handbook, Information Security (Sept. 2016)
- FFIEC, IT Examination Handbook, Retail Payment Systems (Apr. 2016)
- FFIEC, IT Examination Handbook, Supervision of Technology Service Providers (Oct. 2012)

FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005); FFIEC, *Supplemental to Authentication in an Internet Banking Environment* (June 28, 2011)

FFIEC, *Cybersecurity Assessment Tool (CAT)* (June 2015): The CAT is a support tool issued by the FFIEC to assist financial organizations with managing cyber-risk. CAT is strongly encouraged by some US states, but in general it is based on existing guidance and thus does not constitute new regulation.

Gramm-Leach-Bliley Act (1999), 15 U.S.C. § 6801 *et seq.;* **Regulation P, Privacy of Consumer Financial Information** 12 CFR 1016.1 et seq.; – enacted to control how financial institutions manage the private information of individuals. In addition, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information include provisions associated with the role of risk management, boards and third party oversight.

Durbin Amendment, 15 U.S.C. § 1693o-2; 12 CFR § 235.1 *et seq.* (interchange transaction fees)

Federal Trade Commission Act (1914), 15 U.S.C. § 45(a) (prohibiting "unfair or deceptive acts or practices in or affecting commerce"); 16 CFR § 314.3 (requiring companies to develop written information security programs to protect customer information)

Consumer Financial Protection Act of 2010, 15 U.S.C. § 5531 *et seq.* (prohibiting "unfair, deceptive, or abusive act[s] or practice[s]. . ." in consumer finance)

State-based cybersecurity and breach laws: A challenge due to the variation among those sets of regulation which include:

- All 50 States address unauthorized access, malware and viruses
- 20 States address spyware
- 23 States address phishing

Source: National Conference of State Legislatures

International cybersecurity regulations and related data-protection laws: Vary widely and continue to evolve; e.g. European Union General Data Protection Regulations (May 2018); *Japan:* The Act on the Protection of Information (May 2017)

Office of Foreign Assets Control (OFAC)/Sanction Screening

OTHER REFERENCES

ANSI X9.8-1 Personal Identification Management (PIN) Management and Security
Part 1: PIN protection principles and techniques for online PIN verification in ATM & POS systems (equivalent of ISO 9564)

- Applicable to institutions responsible for implementing, managing, and protecting PINs
- Provides the minimum security measures required for effective international PIN management (ATM and POS)
- Includes PIN protection techniques applicable to card payments initiated in an online environment
- Provides a standard means of interchanging PIN data

ISO 9564 Banking Personal Identification Number (PIN) Package

- Provides businesses, government agencies, and other organizations with tools needed to protect against the theft and misuse of personal and financial information
- The requirements in this document are intended to apply in addition to applicable Payment Card Industry Data Security Standard (PCI DSS) requirements to the token data environment (TDE). The TDE is a dedicated, secure area within the token service provider (TSP), where one or more of the following services are performed:
  - Token generation, issuing, and mapping processes
  - Assignment of token usage parameters
  - Token lifecycle management
  - Processes to map or re-map tokens, or perform de-tokenization
  - Cryptographic processes to support tokenization functions
  - Maintenance of underlying token security and related processing controls, such as domain restrictions during transaction processing
- Covers management and security requirements for online / offline PIN handling in ATM and POS systems
- Includes algorithms for PIN encipherment and open network PIN handling

ANSI X9.24-1 Retail Financial Services Symmetric Key Management
Part 1: Using Symmetric Techniques

- Specifies minimum requirements for the management of keying material
- Covers manual and automated management of keying material used for financial services such as point of sale (POS) transactions and automatic teller machine (ATM) transactions; messages among terminals and financial institutions; interchange messages among acquirers, switches, and card issuers
- Deals exclusively with management of symmetric keys using symmetric techniques
- This part of this standard does not cover message format, communications protocol, transmission speed, or device interface

ANSI X9.24-2 Retail Financial Services Symmetric Key Management
Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

- Covers manual and automated management of keying material used for financial services such as point of sale (POS) transactions and automatic teller machine (ATM) transactions; messages among terminals and financial institutions; interchange messages among acquirers, switches and card issuers
- May apply to internet-based transactions, but only when such applications include the use of a tamper resistant security module (TRSM) as defined in section 7.2 of ANS X9.24 Part 1 to protect the private and symmetric keys
- Deals with management of symmetric keys using asymmetric techniques and storage of asymmetric private keys using symmetric keys

ISO/IEC 7816-4 Identification cards – Integrated circuit cards
Part 4: Organization, security and commands for interchange

- Independent from the physical interface technology
- Applies to cards accessed by one or more of the following methods: contacts, close coupling, radio frequency

ANSI X9.122 Secure Customer Authentication for Internet Payments – draft in approval stage
(Note: It says that to use PIN you must use the standards already referenced in PIN)

- Requirements for secure customer authentication for electronic payment transactions over multiple channels initiated through the interchange system (debit/credit network) via internet, mobile or voice channels
- Includes requirements for passcodes, passwords, biometrics, magnetic stripe authentication values, cryptography, small device authentication, and vendor considerations

Protection of Sensitive Payment Card Data through Encryption
ANSI ASC X9.119 Retail Financial Services - Requirements for Protection of Sensitive Payment Card Data

- Part 1: Using Encryption Methods - defines minimum security requirements when employing encryption methods to protect sensitive payment card data. "Protection" refers to maintaining the secrecy of the data from unauthorized disclosure. It applies to protection of the data from the point of encryption to the point of decryption, wherever those points may be in a given system. Addresses the protection of sensitive payment card data from the requesting entity to the token request interface.
- Part 2: Implementing Post-Authorization Tokenization Systems standard focuses on the tokenization service and the token request interface. It defines the minimum security requirements when employing a post-authorization tokenization system to protect sensitive payment card data. "Protection" refers to maintaining the secrecy and integrity of the data protected by tokenization from unauthorized disclosure and modification. Data encryption, integrity protection, and the support for key management services are required to protect sensitive payment card data during the tokenization and de-tokenization process.

ISO Information Technology – Encryption Algorithms

- ISO/IEC 10116 – Security techniques – Modes of operation for an n-bit block cipher - These modes provide methods for encrypting and decrypting data where the bit length of the data may exceed the size of the block cipher and provide protection of data confidentiality.
- ISO/IEC 18033-2 – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers – Encryption (or encipherment) techniques protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to plaintext or cleartext data to yield encrypted data (or ciphertext). The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Every encryption algorithm has a corresponding decryption algorithm, which transforms ciphertext back into its original plaintext. An asymmetric, i.e. public-key, encryption scheme allows a sender to use a recipient's public key to transmit an encryption of a message to the receiver, who uses his secret key to decrypt the given ciphertext to obtain the original message.
- ISO/IEC 18033-3 – Security techniques – Encryption algorithms – Part 3: Block ciphers – A block cipher is a symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext. The following algorithms are specified in this standard:
  - 64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT
  - 128-bit block ciphers: AES, Camellia, SEED

ANSI ASC X9.97 Secure Cryptographic Devices (Retail)

- Part 1: Concepts, Requirements and Evaluation Methods – incorporates the cryptographic processes defined in ISO 9564, ISO 16609 and ISO 11568. Part 1 has two primary purposes:
  - To state the requirements concerning both the operational characteristics of secure cryptographic devices (SCDs) and the management of such devices throughout all stages of their life cycle
  - To standardize the methodology for verifying compliance with those requirements
- Part 2: Security Compliance Checklists for Devices Used in Financial Transactions - Identical to ISO 13491, which specifies use of checklists to evaluate SCDs incorporating cryptographic processes, as specified in parts 1 and 2 of ISO 9564, ISO 16609 and parts 1 to 6 of ISO 11568, in the financial services environment. IC payment cards are subject to the requirements identified in this part of ISO 13491 up until the time of issue, after which they are regarded as a "personal" device and outside of the scope of this document.

ISO 13491 Banking – Secure cryptographic devices, all parts

Key Management Schemes
ANSI Accredited Standards Committee

ANSI Accredited Standards Committee
- X9.44 – Key Establishment Using Integer Factorization Cryptography - RSA - Integer Factorization Cryptography
- X9.133 – Identity Based Encryption for Financial Services Industry (in drafting stage) - Encryption algorithms used to attain standard levels of cryptographic strength when using the identity of a user (or application) as the public key, as banks often do.
- X9.42 –- Public Key Cryptography for Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography - Diffie-Hellman - Discrete Logarithm Cryptography. Adapted from ISO 11770-3.
- X9.98 – Lattice-Based Polynomial Public Key Encryption Algorithm Part 1: Key Establishment
- X9.63 – Key Agreement and Key Management Using Elliptic Curve-Based Cryptography - Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques
- TR 34 Part 1 – Using Factor Based Public Key Cryptography Unilateral Key Transport
- TR 31 – Interoperable Secure Key Exchange Key Block Specifications for Symmetric Algorithms

ISO 11770-3 Information technology – Security techniques – Key management –
Part 3: Mechanisms using asymmetric techniques

Key Management Methods
ANSI Accredited Standards Committee

- X9.102-2008 Key Wrap Standard – for symmetric key block ciphers whose block size is either 64 bits or 128 bits
- X9.69-2012 Framework for Key Management Extensions- Symmetric cryptographic algorithms - Key extensions
- X9.79-4-2013 Public Key Infrastructure – Part 4: Asymmetric Key and Public Key Infrastructure
- X9.24 Retail Financial Services Symmetric Key Management
  - Part 1- Symmetric Key Management
  - Part 2- Using Asymmetric Techniques for the Distribution of Symmetric Keys
  - Part 3- Derived Unique Key per Transaction (AES-DUKPT) Symmetric Key Management using AES DUKPT. This is the new standard replacing Triple DES – TDEA.
- TR-34-1-2012 Interoperable Method for Distribution of Symmetric Keys using Asymmetric techniques – Part 1 Using Factor Based Public Key Cryptography Unilateral Key Transport – Technical Report provides guidelines for secure exchange of keys using asymmetric techniques between two devices that share asymmetric keys.
- ISO 15782 (similar to ISO X9.79-4) Certificate management for financial services – Part 1: Public key certificates - defines a certificate management system for financial industry use for legal and natural persons that includes credentials and certificate contents, certification authority systems, including certificates for digital signatures and for encryption key management certificate generation, distribution, validation and renewal, authentication structure and certification paths, and revocation and recovery procedures. Also recommends some useful operational procedures.

Format Preserving Encryption

- ANSI ASC X9.124 Format Preserving Encryption of Financial Information – Format preserving encryption is useful in situations where fixed-format data, such as primary account numbers or Social Security numbers, must be encrypted, but there is a requirement to limit changes to existing communication protocols, database schemata or application code. Format Preserving Encryption Counter Mode is a particularly simple and efficient mechanism to achieve format preserving encryption, which shares many of the strengths and challenges of Counter Mode (CTR) as defined in NIST SP38B.
  - Part 1 Cryptographic algorithms – Block Ciphers — covers format preserving block ciphers
  - Part 2 Cryptographic algorithms – Stream Ciphers – covers format preserving stream ciphers
- NIST SP 38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication – This recommendation specifies a message authentication code (MAC) algorithm based on a symmetric key block cipher. This block cipher-based MAC algorithm, called CMAC, may be used to provide assurance of the authenticity and, hence, the integrity of binary data.

ANSI TR-39/TG-3 Frequently Asked Questions

- When this guideline is completed by a device manufacturer, the control objectives are intended to evaluate the PIN key management environment and device's ability to be implemented in a manner compliant with X9.8 and X9.24 (all parts)
- Applies to all organizations using Triple Data Encryption Algorithm (TDEA) for encryption of PINs used for retail financial services: point of sale (POS) transactions and automatic teller machine (ATM) transactions; messages among terminals and financial institutions; interchange messages among acquirers, switches and card issuers
- This guideline/checklist should be completed by all organizations acquiring or processing transactions containing PINs, from the terminal driving system to authorizing entity
- Control objectives address security controls of from PIN entry device to interface delivering transaction to authorizing entity
- Control objectives address security controls of PIN key management full life cycle from creation, distribution, loading and deletion

ANSI X9.122 Secure Customer Authentication for Internet Payments – draft in approval stage
(Note: It says that to use PIN you must use the standards already referenced in PIN)

- Covers passcodes, passwords, biometrics, magnetic stripe authentication values, cryptography, small device authentication, and vendor considerations
- Requirements for secure customer authentication for electronic payment transactions over multiple channels initiated through the interchange system (debit/credit network) via internet, mobile or voice channels

"Best Practice" Implementation for ATM Operators

EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3

Source: https://www.emvco.com/emv-technologies/contact

EMV Payment Tokenization Specification – Technical Framework

- Payment tokens are surrogate values that replace the Primary Account Number (PAN) in the payments ecosystem. They may be used to originate payment transactions, while non-payment tokens may be used for ancillary processes, such as loyalty tracking. This specification does not address non-payment tokens, but does not preclude their use.

Source: https://www.emvco.com/

Payment Card Industry (PCI) Data Security Standard (PCI DSS) – Requirements and Security Assessment Procedures

- Developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. It provides a baseline of technical and operational requirements designed to protect account data and applies to all entities involved in payment card processing including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Source: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3 2.pdf?agreement=true&time=1484000182971

Payment Card Industry (PCI) Point-to-Point-Encryption – Encryption, Decryption, and Key Management within Secure Cryptographic Devices (Hardware/Hardware)

- Provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this version contains validation requirements and testing procedures for hardware-based encryption and decryption solutions, also called "hardware/hardware." Hardware/hardware solutions utilize secure cryptographic devices for both encryption and decryption including at the point of merchant acceptance for encryption, and within hardware security modules (HSMs) for decryption.

Payment Card Industry (PCI) Point-to-Point-Encryption – Encryption and Key Management within Secure Cryptographic Devices, and Decryption of Account Data in Software (Hardware/Hybrid)

- Provides a method for providers of P2PE solutions to validate their solutions, and for merchants to reduce the scope of their PCI DSS assessments when using a validated P2PE solution for account data acceptance and processing. Specifically, this version contains validation requirements and testing procedures for hardware/hybrid solutions which utilize secure cryptographic devices at the point of merchant acceptance for encryption and for managing cryptographic keys in the decryption environment while utilizing non-SCDs for the decryption of account data.

Payment Card Industry (PCI) Token Service Providers – Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens)

Payment Card Industry (PCI) Payment Application Data Security Standard (PCI PA-DSS) – Requirements and Security Assessment Procedures

- Defines security requirements and assessment procedures for software vendors of payment applications. This document is to be used by Payment Application Qualified Security Assessors (PA-QSAs) conducting payment application assessments to validate that a payment application complies with the PA-DSS.
- Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of primary account number (PAN), full track data, Card Verification Values1, PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Payment Card Industry (PCI) Point-to-Point-Encryption – Solution Requirements and Testing Procedures

- Defines both requirements and testing procedures for Point-to-Point Encryption (P2PE) solutions. The objective of this standard is to facilitate the development, approval, and deployment of PCI approved P2PE solutions that will increase the protection of account data by encrypting that data from the point of interaction within the encryption environment where account data is captured to the point of decrypting that data inside the decryption environment, effectively removing clear-text account data between these two points.
- The requirements contained within this standard are intended for P2PE solution providers and other entities that provide P2PE components or P2PE applications for use in P2PE solutions, as well as P2PE assessors evaluating these entities. Additionally, merchants benefit from using P2PE solutions due to increased protection of account data and subsequent reduction in the presence of clear-text account data within their environments.

Payment Card Industry (PCI) Card Production and Provisioning – Logical Security Requirements

- All systems and business processes associated with the logical security activities associated with card production and provisioning such as data preparation, pre-personalization, card personalization, PIN generation, PIN mailers, and card carriers and distribution must comply with the requirements in this document.
- This document describes the logical security requirements required of entities that:
  - Perform cloud-based or secure element (SE) provisioning services;
  - Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or
  - Manage associated cryptographic keys.

Payment Card Industry (PCI) Card Production and Provisioning – Physical Security Requirements

- A comprehensive source of information for entities involved in card production and provisioning, which may include manufacturers, personalizers, pre-personalizers, chip embedders, data-preparation, and fulfillment.
- The contents of this manual specify the physical security requirements and procedures that entities must follow before, during, and after the following processes:
  - Perform cloud-based or secure element (SE) provisioning services; card manufacturing, chip embedding, personalization, storage, packaging, mailing, shipping or delivery, fulfillment

Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) –
Modular Security Requirements

- Provides vendors with a list of all the security requirements against which their product will be evaluated in order to obtain Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI) device approval.

NIST Cyber security Framework (CSF)

Payment network rules
(e.g. Visa, MasterCard, American Express, Discover Network, JCB and debit card networks)

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

Payments stakeholders employ various methods and processes to comply with relevant state and federal regulations regarding customer onboarding as well as relevant private sector protocols. Greater focus on the development and adoption of standards related to online registration or mobile enrollment could enhance security.

No current standard for migration from Triple DES encryption to AES Derived Unique Key per transaction. With faster computing capacity, Triple DES is no longer sufficiently secure, an issue which X9.24-3 will address, but it is in early drafting stage. Implementing these changes will require significant changes, from terminal to every place in the network, as well as modified fields in the transaction flow, such as new PIN block.

Greater deployment of tokenization, user authentication and encryption based on open standards could enhance payment security.

Improvements to the quality and accuracy of data collected and used to facilitate mail order, telephone order, recurring payments, one-time card on file and card present key entry payments may help further mitigate payments risk. Participants who collect, process, or authorize transactional data play an important role in ensuring the accuracy of data submitted. This includes ensuring that hardware and software are properly configured. Participants may use this information as part of their authentication decision process, making accuracy an important priority.

Greater focus on development and adoption of risk-based cybersecurity rules, frameworks and open standards could enhance security.

PIN standards only address "card present" transactions. Randomized PIN pad functionality provides software-based online PIN entry, but it violates PIN security standards, which require cryptographic hardware for encryption, including X9.24, X9.8, and ISO standards as well as TRS (Telecommunication Relay Services) standards.

Open standards related to PIN capture need to be expanded to include new and evolving forms of PIN entry.

Payment stakeholders are deploying authentication and multiple layers of risk mitigation. Some of these tools include dynamic data, tokens, multi-factor authentication, geolocation, and analytic engines. Greater deployment of such tools may help reduce risk.