SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Wallet

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 Wallet Lifecycle and Security Profile maps out the lifecycle of a wallet payment to establish a common understanding of the payment journey and serves 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).

WALLET

Definition: A payment card (e.g. credit or debit) funded transaction whereby a cardholder leverages a digital container accessed by a mobile device (e.g. a smartphone) that stores wallet applications, tokenized payment credentials, loyalty cards, and coupons and is used to make proximity and remote mobile payments. Tokenized payment credentials are either stored securely in the mobile phone [if near-field communication (NFC)] or in the cloud. Wallet transactions may be completed using NFC "pay" wallets (e.g. Apple Pay, Samsung Pay, Android Pay), cloud-based card-on-file wallets (e.g. PayPal, Pay, Amazon), cloud-based card-on-file card network digital "checkout" wallets (e.g. Express Checkout by American Express, Masterpass, Visa Checkout) and closed-loop merchant or financial institution quick reference (QR) code closed wallets (e.g. Chase Pay, Walmart Pay). These transactions may also have the ability to support biometrics, PIN and signature for consumer authentication.

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

				WALLET **(VIA CONTACTLESS OR IN APP)** Note: For Wallet transactions that leverage Contactless technology, please also refer to the Contactless Payment Lifecycle and Security Profile.
			GENERIC FUNCTIONAL STEP	**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	User provides (or issuer provides in auto-enrollment scenario) participating credit/debit card information with additional personally identifiable information (PII) authentication data to Wallet Service Provider to be verified by issuer to complete provisioning. Final provision incorporates a tokenization request to a token service provider to request a payment token for the previously issued card to be provisioned to wallet. The PIN associated with the account may be communicated to the cardholder via direct outreach, email, or physical mail. For Card Not Present authentication, merchant identifies required information based on relationship with customer; enrollment could mean the cardholder establishes an account or profile with the merchant.
			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.
TRANSACTION	Payer Authentication	**PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS**	**Payer Authentication** Verification of payer when originating payments	Many wallet providers require local device authentication to access the wallet before any payment requests can be initiated. Once payment is initiated, cardholder and card verification methods may include Tokenized Primary Account Number (PAN), expiration date, out-of-band authentication/verification, Dynamic Card Verification Value (dCVV), cryptogram. PIN / Passcode
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	On-premise: NFC/MST/QR Code acquired In-app: Wallet service payment integration with application providers
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	Contactless reader at the Point of Sale (POS), phone, tablet, wearable, PC, Internet of Things (IOT)
			Funding Account for Payment Entry and/or identification of the funding account (with format checks)	Demand Deposit Account (DDA) or credit account
			Payment Initiation Mechanism Payment network, system and/or third-party accessed	Merchant, acquirer, association or network, processor
	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 and debit networks). If tokenized, de-tokenization through Token Service Provider must occur to allow authorization.
			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 within payment network service level agreements (SLAs).
	Format Exchange		**Format Exchange** Payment instructions, rules, and formatting	Payment network rules dictate format exchange.
	Receipt		**Acknowledgement/ Guarantee** Notification and confirmation of payment completion including terms for use	Transaction is confirmed but fulfillment maybe delayed until authorization (guarantee of funds).
	Payee Authentication		**Payee Authentication** Mode of access to funds (or accounts)	Acquirer authenticates merchant.
	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 and debit networks).
RECONCILIATION			**Reconciliation / Exception Handling** Process and responsibilities associated with reconciling and handling any exceptions or problems with a payment	Cardholder is required to report dispute within specified timeframe defined by payment network 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 regulation Regulation Z consumer protections apply to consumer credit and Regulation E applies to 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/payment token to wallet, if applicable. Know Your Customer (KYC), Customer Identification Program (CIP) background checks, etc.; ID verification of a 'carbon-based lifeform' 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. Additional risk scoring and authentication may be performed by the issuer before allowing a card to be enrolled in a wallet (e.g. step-up authentication) Strong key management is also necessary to store and load encryption keys and/or account information on a mobile device.	Social engineering (e.g. call center or end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Account takeover Credential stuffing (e.g. automated injection of breached username/password pairs in order to fraudulently gain access to user accounts) 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. Authenticated yet unauthorized and/or compromised credentials being integrated the payment channel or the device, subsequently used for cash-out at point of sale or payments channel 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 which could lead to a "bust-out" situation. 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		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). Use of data encryption (end-to-end) 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.	Account takeover risk Social engineering (e.g. end user) which could include business email compromise, masquerading fraud, imposter fraud, etc. Machine takeover (payee, financial institutions, network/operator, payer) Transaction data may be intercepted altered or spoofed (e.g. counterfeit transactions, credit master attacks, brute force attacks, etc.). Imposter apps/mobile apps/third party/contactless emulation may be used to compromise account data (PAN expiry) and used in contactless environment. First party/theft/lost or stolen transactions Credential stuffing (e.g. automated injection of breached username/password pairs in order to fraudulently gain access to user accounts) Sole reliance on a point in time compliance statement (minimal, "check the box" compliance does not equal security) Some POS systems transmit and/or store card data in the clear. End-to-end encryption is not universally applied in POS systems. Issuer must use all discretionary card fields to validate consumer. For instance, there are methods of duplicating EMV Chip transactions but the encryption fails -- some issuers were accepting them anyway. Authenticated yet unauthorized and/or compromised credentials being integrated the payment channel or the device, subsequently used for cash-out at point of sale or payments channel The speed of payment processing and reconcilement may impact the ability to identify fraud in time to recover funds. Inadequately-controlled enrollment often poses additional risk at the time of transaction.
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Participants in the original payment transaction may utilize anomaly and fraud detection tools to identify suspicious patterns of activity which 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	Sensitive data used to enroll a card or open a wallet account: Card Number | Expiration Date | Card Verification Values[1] | Name | Address | Zip Code | Phone Number | Email address Additional sensitive data exchanged during token provisioning: Name | Address | PAN | Expiration Date | CAV2/ CVC2/CVV2/CID	If compromised, data can be used to make transactions via the wallet, create a counterfeit card, and be used for other identity theft crimes. Card may be fraudulently provisioned into unauthorized user's wallet. Compromised device may be used to make fraudulent wallet purchases. Compromised emails and mobile phone numbers can open up fraud through phishing-type attacks.
	PAYEE ID / ENROLLMENT	Sensitive data used to enroll or open a merchant account: Name | Date of Birth | Address | Social Security Number | Demand Deposit Account Number (DDA) | Signature | Business Name | Tax ID Terminal information (IDs, entry capability, etc.)	Onboarding Merchant: 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		Payment Token Data: Token Token expiration date Token type Dynamic Card Verification Value (dCVV)/Chip Card Security Code (e.g. iCVV, CHIP CVC, iCSC) Card sequence number Card type Card PIN (encrypted/offset) Service code Velocity limits Signature Biometric parameters Device / Form Factor credentials and IDs PIN **The following data is considered Sensitive Payment Data:** Cardholder Data: *Cardholder data must be protected wherever it is processed, stored or transmitted* Primary Account Number (PAN) Cardholder Name Expiration Date Service Code Signature Sensitive Authentication Data: *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	If compromised, data can be used to fraudulently set up an account at a financial institution and be used for other identity theft crimes. If this information is compromised during token provisioning, card information can be used to make fraudulent card not present transaction
	PAYEE AUTHENTICATION	During transaction flow: Merchant ID | Terminal ID | Terminal address | Merchant Category Code (MCC) | Terminal country code | Transaction currency code | Transaction type | Terminal entry capability | Merchant name	During transaction flow: If compromised, 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, data may be used to make fraudulent debits to the settlement accounts
RECONCILIATION	RECONCILIATION / EXCEPTION HANDLING	Varies by transaction type/governing body: Acquirer reference number | Token | Token status | Transaction date/time | Merchant name | Transaction amount Chargeback reason code	If compromised, someone that is not a merchant could spoof a legitimate merchant.
	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

Note: See the Regulations section for the applicable funding method (e.g., ACH, credit or debit card).

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.*

FFIEC MFC Guidance (for safe mobile applications)

- MFA and re-authentication
- Maintenance – annual mobile application testing
- Use of geo-location for fraud control, transaction monitoring
- Open Web Application Security Project (OWASP) standards

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, Wholesale Payment Systems (July 2004)
- 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
- Covers management and security requirements for online / offline PIN handling in ATM and POS systems

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
- Covers passcodes, passwords, biometrics, magnetic strip 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

- 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 bit
- 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.

SimAlliance (NFC with HCE or secure element) Access mode/network credit/debit

- Protection of payment credentials
- Communications between mobile device and POS terminal

GSMA NFC Core Wallet Requirements and Mobile Wallet WP (NFC with HCE or secure element) credit/debit

- Protection of payment credentials
- Communication between mobile device and POS terminal
- Includes algorithms for PIN encipherment and open network PIN handling

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 does preclude their use.

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

EMV QR Code Specification for Payment Systems – Consumer-Presented Mode Version 1.0 and the EMV QR Code Specification for Payment Systems Merchant-Presented Mode Version 1.0

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

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) 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 Values[1], 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 through 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) 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) 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) 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.

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

- The requirements in this document are intended to apply in addition to applicable PCI DSS requirements to the token data environment (TDE). The TDE is a dedicated, secure area within the 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.

Global Platform Specifications for secure/interoperable deployment and management of applications on SE, TEE (NFC with secure element or TEE) Access mode/network credit/debit

- Protection of payment credentials
- http://www.global platform.org
- European Payments Council (EPC) credit and debit
- EPC492-09 Mobile Payments WP
- EPC178-10 Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines
- http://www.europeanpaymentscouncil.eu

Mobey Forum (global back focused) analysis and education on mobile wallets (NFC with secure elements) Access mode/network credit/debit

- Protection of payment credentials
- Communications between mobile device and POS terminal

NIST Cybersecurity Framework (CSF) and Sector-specific variations (Profiles) under development by leading financial services organizations. The CSF was mandated under and Executive Order 13636 in February of 2013 and has had significant domestic and international influence on not only the standardization of cybersecurity practices, but also on regulatory oversight activities. The CSF remains a voluntary standard, but regulators strongly encourage its use and adoption.

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

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

Tokens have the opportunity to improve security in the payments ecosystem, and standards would enable more interoperability and the use of tokens in various applications.

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.

The market has evolved to offer different kinds of mobile/digital wallets models. These models may vary in authentication, enrollment, use of tokenization, etc. They can be roughly categorized as the following types: NFC Pay Wallet (e.g., Apple Pay, Android Pay, Samsung Pay), cloud-based wallets with QR codes for POS contactless payments (e.g., Chase Pay, Walmart Pay), eCommerce wallets with Guest checkout, eCommerce wallets with card on file (e.g., Amazon, PayPal), digital checkout wallets provided by card networks (e.g., Visa Checkout, Masterpass, American Express Express); and in-app mobile application wallets (i.e. iTunes and others to access special content or features in a video).

Each wallet accepts a mix of payment methods but not all of the mixes are the same: depends on the wallet type.

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

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

Continued development and evolution of best practices for validating card credentials stored in a digital/ mobile wallet may help enhance security.