SECURE PAYMENTS TASK FORCE

PAYMENT LIFECYCLE AND SECURITY PROFILE: Contactless

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 Contactless Payment Lifecycle and Security Profile maps out the lifecycle of a contactless 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).

CONTACTLESS

Definition: A payment card (e.g. credit or debit) funded transaction whereby the cardholder typically presents a physical smart card (e.g. credit or debit card), key fob, or a mobile device or wearable (e.g. smartphones, smart watches) where the payment data is exchanged by placing the payment device in proximity of the point of sale to complete the transaction.

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

CONTACTLESS

[Near Field Communications (NFC), Magnetic Stripe Data (MSD), Host Card Emulation (HCE), Bluetooth, Quick Response (QR) Code, Magnetic Secure Transmission (MST)]

Note: For Contactless transactions where the cardholder presents a mobile device or wearable, please also refer to the Wallet 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	Individual or organization requests account with issuer. Issuer verifies customer information in accordance with their Know Your Customer (KYC) program. 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
TRANSACTION	Payer Authentication	PAYMENTS/TRANSFERS FLOW IN BOTH DIRECTIONS	**Payer Authentication** Verification of payer when originating payments	Cardholder and card verification methods include Primary Account Number (PAN), expiration date, Dynamic Card Verification Value (DCVV), out-of-band authentication/verification, Application Transaction Counter (ATC) with additional cardholder verification potentially required based on transaction request amount, EMV Application Cryptogram.
	Initiation		**Access Mode / Network** Environment in which the payment origination is requested	Point Of Sale (POS), in-person
			Device/Method Used to Initiate Payment Type of interaction or device used to enter payment account information	Contactless reader or scanner at the Point of Sale (POS), contactless form factor (e.g. card, sticker, mobile device, wearable etc.)
			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	Online authorization occurs through payment networks (e.g. credit and 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 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 may be 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	Disputes are required to be reported/processed 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 an account. 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 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. Knowledge-based questions can be compromised
	PAYEE ID / ENROLLMENT	Acquirer (or the agent of the acquirer) verifies the individual(s) or organization 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 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 initiation 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.	Using Primary Account Number (PAN) for part of the remaining processes (these are keys to access money) Imposter apps/mobile apps/third party/contactless emulation may be used to compromise account data (PAN expiry) and used in contactless environment. Interception of contactless transmission 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 altered or spoofed (e.g. counterfeit transactions, credit master attacks, brute force attacks, etc.). 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/applications transmit and/or store card data in the clear. End-to-end encryption is not universally applied in POS systems/applications. Timely contactless authentication methods may not exist in the U.S. 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	Sensitive data used to enroll or open an account: Name | Date of Birth | Address | Zip Code | Social Security Number | Demand Deposit Account Number (DDA) | Signature Sensitive data used during token provisioning: Name | Address | PAN | Expiration Date | CAV2/CVC2/CVV2/CID	If compromised, 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	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. ICCV, 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 **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] (at this point the token is re-associated with the card PAN by the token service provider and sent to issuer) 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 | MCC | 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

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 (BSA)/Anti-Money Laundering (AML) compliance, Bank Secrecy Act, 31 U.S.C. § 5311, *et. seq.;* 31 CFR § 1010.100, et seq. (implementing regulations); Federal Financial Institutions Examination Council (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

ISO/IEC 13157 Information technology – Telecomm and information exchange between systems – NFC Security Parts 1-5:

- Part 1: NFC-SEC NFCIP-1 security services and protocol (ISO/IEC 13157-1:2014)
  - Specifies the NFC-SEC secure channel and shared secret services for NFCIP-1 and the Protocol Data Units and protocol for those services
- Part 2: NFC-SEC cryptography standard using ECDH and AES (ISO/IEC 13157-2:2016)
  - Specifies the message contents and the cryptographic methods for PID 01
  - Specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity
- Part 3: NFC-SEC cryptography standard using ECDH-256 and AES-GCM (ISO/IEC 13157-3:2016)
  - Specifies the message contents and the cryptographic methods for PID 02
  - Specifies cryptographic mechanisms that use the Elliptic Curves Diffie-Hellman (ECDH) protocol with a key length of 256 bits for key agreement and the AES algorithm in GCM mode to provide data authenticated encryption
- Part 4: NFC-SEC entity authentication and key agreement using asymmetric cryptography
  - Specifies the message contents and the cryptographic mechanisms for PID 03
  - Specifies key agreement and confirmation mechanisms providing mutual authentication, using asymmetric cryptography, and the transport protocol requirements for the exchange between Sender and TTP
  - Adds entity authentication to the services provided by ISO/IEC 13157-3 (ECMA-409) NFC-SEC-02
- Part 5: NFC-SEC entity authentication and key agreement using symmetric cryptography
  - Specifies the message contents and the cryptographic mechanisms for PID 04.
  - Specifies key agreement and confirmation mechanisms providing mutual authentication, using symmetric cryptography.
  - Adds entity authentication to the services provided by ISO/IEC 13157-3 (ECMA-409) NFC-SEC-02

ANSI X9.112 Wireless Management and Security

- Part 1: General Requirements addresses:
  - Risks related to wireless systems and legacy networks opened by the wireless environment are described in §5 Wireless Risks
  - Requirements for managing wireless systems in a secure fashion are defined in §6 Requirements
  - Requirements for policy management are defined in §7 Wireless Security Policy
  - Control objectives for evaluating wireless systems are provided in Annex A: Wireless Validation Control Objectives
  - Information regarding cryptography relating to wireless technology is provided in Annex B: Wireless Cryptography Controls
  - Background information on other wireless standards is provided in Annex C: Wireless Technology Standards
  - Other wireless-related standards recognized by X9 are listed in Annex D: X9 Registry
- Part 2: POS and ATM addresses the following:
  - End-to-end encryption to protect transactional and operational information from unauthorized entities
  - Patches and modification management to protect systems from vulnerabilities
  - Configuration management to protect wireless systems from weaknesses
  - Physical and logical security controls to protect wireless access
  - Network segmentation to protect against attacks originating from wired and wireless environments
  - Monitoring controls to detect threats from higher risk environments

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

- Protection of payment credentials

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

- Protection of payment credentials

ISO/IEC 13239: 2002 Information technology – Telecomm & information exchange between systems – High-level data link control (HDLC) procedures

ISO/IEC 18092: 2013 Information technology – Telecomm and information exchange between systems – NFC – Interface and Protocol (NFCIP-1)

- Defines communication modes for NFC interface and protocol (NFCIP 1) using inductive coupled devices operating at the center frequency of 13,56 MHz for interconnection of computer peripherals
- Defines active and passive communication modes of NFC interface and protocol (NFCIP-1) to realize a communication network using NFC devices for networked products and consumer equipment
- Specifies modulation schemes, coding, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization
- Defines a transport protocol including protocol activation and data exchange methods

ISO/IEC 16353: 2011 Information technology – Telecomm and information exchange between systems – Front-end configuration command for NFC-WI (NFC-FEC)

- Specifies commands for the NFC Wired Interface (NFC-WI) specified in ISO/IEC 28361. The commands allow exchange of control and state information between the transceiver and the front-end.

ISO/IEC 28361: 2007 Information technology – Telecomm and information exchange between systems – NFC Wired Interface (NFC-WI)

- Specifies the digital wire interface between a transceiver and a front-end
- Includes the signal wires, binary signals, the state diagrams and the bit encodings for three data rates
- ISO/IEC 7816 Identification cards – Integrated circuit cards Parts 1-15:
  - Part 1: Cards with contacts – Physical characteristics
  - Part 2: Cards with contacts – Dimensions and location of the contacts
  - Part 3: Cards with contacts – Electrical interface and transmission protocols
  - Part 4: Organization, security and commands for interchange
  - Part 5: Registration of application providers
  - Part 6: Inter-industry data elements for interchange
  - Part 7: Inter-industry commands for Structured Card Query Language (SCQL)
  - Part 8: Commands and mechanisms for security operations
  - Part 9: Commands for card management
  - Part 10: Electronic signals and answer to reset for synchronous cards
  - Part 11: Personal verification through biometric methods
  - Part 12: Cards with contacts – USB electrical interface and operating procedures
  - Part 13: Commands for application management in a multi-application environment
  - Part 15: Cryptographic information application

NIST Cybersecurity Framework (CSF)

EMV Contactless Specifications for Payment Systems

- Book A: Architecture and General Requirements - defines a generalized POS System environment that includes:
  - Reader functionality
  - Terminal functionality
  - Entry point software that performs the initial analysis of a contactless transaction and invokes appropriate kernel software, and
  - Several kernels, each of which provides processing appropriate to certain contactless transactions.
- Book B: Entry Point -defines the reader requirements necessary to support a multi-kernel architecture that enables:
  - Discovery and selection of a contactless application that is supported by both the
  - Reader and the card
  - Activation of the appropriate kernel for processing the contactless transaction in an international interchange environment
  - NOTE: this specification is based on the ISO/IEC 7816 and ISO/IEC 14443 series of standards and should be read in conjunction with those standards
- Books C [C-1, C-2, C-3, C-4, C-5, C-6, C-7]: Kernel Specifications
- Book D: Contactless Communication Protocol
  - Describes the minimum functionality required of proximity integrated circuit cards (piccs) and proximity coupling devices (pcds) to ensure correct operation and interoperability independent of the application to be used. Additional proprietary functionality and features may be provided, but these are beyond the scope of this specification and interoperability cannot be guaranteed. This specification is intended for use by manufacturers of piccs and pcds, system designers in payment systems, and financial institution staff responsible for implementing financial applications in piccs and pcds.

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/

EMV Contactless Mobile Payment – Application Activation User Interface; EMV Mobile Payment: Software-based Mobile Payment Security Requirements; EMV Proximity Payment System Environment (PPSE) and Application Management for Secure Elements

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

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 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 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) Token Service Providers – 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.

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

- Manual is 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

NFC Forum

Source: http://members.nfc-forum.org/specs/spec_list/

Near Field Communication.org

Source: http://nearfieldcommunication.org/payment-systems.html

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

CHALLENGES AND IMPROVEMENT OPPORTUNITIES

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.

Security standards for contactless are evolving in the marketplace in light of the deployment of new technologies (e.g., QR codes, beacons, wearable internet of things).

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.

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.