# Contactless Payment Use Case (DRAFT)

The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

## Contactless

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) that use radio-frequency identification (RFID) or near field communications (NFC) at the point of sale to complete the transaction. These types of transactions can support both pin and signature based consumer authentication techniques for added security.

### 1) Payment Flow Overview

<table>
<thead>
<tr>
<th>Enrollment</th>
<th>Payer Authentication</th>
<th>Initiation</th>
<th>Transaction</th>
<th>Payer Authorization</th>
<th>Format Exchange</th>
<th>Receipt</th>
<th>Payee Authentication</th>
<th>Clearing and Settlement</th>
<th>Reconciliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic functional step or operational role in end-to-end payments value chain</td>
<td></td>
<td></td>
<td>Payments/Transfers Flow in both directions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID proofing, management of users (Enrollment, De-enrollment &amp; Changes) and authority based on role</td>
<td>ID proofing and vetting of participant; management of lifecycle</td>
<td>Verification of payer when originating (or receiving) payments</td>
<td>The environment in which payment origination is requested</td>
<td>Type of interaction or device used to enter payment account information</td>
<td>Entry and/or identification of funding account (with format checks)</td>
<td>Network, system and/or 3rd party accessed</td>
<td>“Rails” used to route authorization requests to holder of funding account</td>
<td>Approval/ decline (and recourse) decision, time-frame, oblivations</td>
<td>Payment Instructions, rules and formatting</td>
</tr>
</tbody>
</table>

### 2) Payment Type Operation

**Contactless (Near Field Communication (NFC), Bluetooth, Quick Response (QR) Code, Magnetic Secure Transmission (MST))**

<table>
<thead>
<tr>
<th>Cardholder verification methods include Primary Account Number (PAN), expiration date, Dynamic Card Verification Value (DCVV), Application Transaction Counter (ATC) with additional cardholder potentially required based on transaction request amount</th>
<th>In-person</th>
<th>Merchant</th>
<th>Online authorization occurs through Payment Networks (e.g. Credit and Debit Networks)</th>
<th>Transactions are approved or declined within Payment Network Service Level Agreements (SLAs)</th>
<th>Payment Network rules dictate format exchange</th>
<th>Transaction is confirmed but fulfillment maybe delayed until authorization (guarantee of funds)</th>
<th>Acquirer authenticates merchant</th>
<th>Settlement occurs per Payment Network rules (e.g. Credit and Debit Networks)</th>
<th>Disputes are required to be reported/processed within specified timeframe defined by Payment Network rules and law</th>
<th>Determined by Payment Network rules and applicable consumer protection laws and regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer verifies customer information</td>
<td>Acquirer approves merchant</td>
<td>Contactless reader at the Point of Sale (POS), contactless form factor (e.g. card, sticker, wearable etc.)</td>
<td>Demand Deposit Account (DDA) or credit account</td>
<td>Transaction is confirmed but fulfillment maybe delayed until authorization (guarantee of funds)</td>
<td>Payment Network rules dictate format exchange</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2017 Federal Reserve Banks. Materials are not to be used without consent.
The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

### 3) Overview of Security Methods and Associated Risks

<table>
<thead>
<tr>
<th>Security Methods</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutions using knowledge-based questions for enrollment (encourages identity theft)</td>
<td>Using Primary Account Number (PAN) for part of the remaining processes (these are keys to access money)</td>
</tr>
<tr>
<td></td>
<td>Mobile apps/third party/contactless emulation may be used to compromise account data (PAN expiry) and used in contactless environment</td>
</tr>
<tr>
<td></td>
<td>Interception of contactless transmission</td>
</tr>
</tbody>
</table>

### 4) Inventory of Sensitive Payment Data and Associated Risks

<table>
<thead>
<tr>
<th>Sensitive Payment Data</th>
<th>Payment Token Data</th>
<th>Sensitive Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>token expiration date</td>
<td>Full track data (magnetic stripe data or equivalent on a chip)</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Dynamic Card Verification Value (dCVV)/CHIP Card Security Code (e.g. ICVV, CHIP CVC, ICSC)</td>
<td>Card Verification Values - CAV2/CAV2/CVV2/CVV2/00/00</td>
</tr>
<tr>
<td>Zip Code</td>
<td>card sequence number</td>
<td>[at this point the token is re-associated with the card PAN by the token service provider and sent to issuer]</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>card type</td>
<td>PIN/PIN Blocks</td>
</tr>
<tr>
<td>Security</td>
<td>velocity limits</td>
<td>Encryption Keys</td>
</tr>
<tr>
<td>Demand</td>
<td>signature</td>
<td>PIN Offsets</td>
</tr>
<tr>
<td>Deposit</td>
<td>Biometric parameters</td>
<td></td>
</tr>
<tr>
<td>Account Number (DDA)</td>
<td>Device / Form Factor credentials and IDs</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensitive data used during token provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Primary Account Number (PAN)</td>
<td></td>
</tr>
<tr>
<td>Business Name</td>
<td>Cardholder Name</td>
<td></td>
</tr>
<tr>
<td>Tax ID</td>
<td>Expiration Date</td>
<td></td>
</tr>
<tr>
<td>Terminal information (IDs, entry capability, etc.)</td>
<td>Service Code</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expiration Date CAV2/CVV2/CVV2/00/00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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

#### Varies by transaction type/governing body:
- acquiring reference 
- token status 
- transaction date 
- MCC 
- merchant name 
- transaction amount 
- chargeback reason code

The following data is considered Sensitive Payment Data:

#### Cardholder Data:
1. Cardholder Data must be protected wherever it is processed, stored or transmitted

#### Sensitive Authentication Data:
2. Sensitive Authentication Data must be protected and must not be stored after authorization of the transaction
The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

### Overview of Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Open Standards:</th>
</tr>
</thead>
</table>
- Specifies the NFC-SEC secure channel and shared secret services for NFCP-1 and the Protocol Data Units and protocol for those services  
- 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  
- 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 |

© 2017 Federal Reserve Banks. Materials are not to be used without consent.
The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes:

1) Payment Flow Overview
2) Payment Type Operation
3) Overview of Security Methods and Associated Risks
4) Inventory of Sensitive Data and Associated Risk
5) Overview of Standards


Part 2: POS and ATM addresses the following:
- End-to-end encryption to protect transactional and operational information from unauthorized entities
- Patch 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) 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
- Defines 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

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

© 2017 Federal Reserve Banks. Materials are not to be used without consent.
# Contactless Payment Use Case (DRAFT)

The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes 1) Payment Flow Overview 2) Payment Type Operation 3) Overview of Security Methods and Associated Risks 4) Inventory of Sensitive Data and Associated Risk 5) Overview of Standards

## Proprietary Standards

  - 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.

  - The PCI Payment Application Data Security Standard (PA-DSS) Requirements and Security Assessment Procedures define 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 PA-DSS-compliant environment, will minimize the potential for security breaches leading to compromises of primary account number (PAN), full track data, card verification codes and values (CVV2, CID, CVC2, CV21), 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**
  - This document, 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)**
  - This document for point-to-point encryption solutions 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/Software)**
  - This document for hardware/hybrid point-to-point encryption solutions 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;
Contactless Payment Use Case (DRAFT)

The Contactless Payment Use Case maps out the lifecycle of a Contactless Payment to establish a common understanding of the payment journey and serve as an educational reference guide to payment/security practitioners. Payment Use Case information includes:
1) Payment Flow Overview
2) Payment Type Operation
3) Overview of Security Methods and Associated Risks
4) Inventory of Sensitive Data and Associated Risk
5) Overview of Standards

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Manage over-the-air (OTA) personalization, lifecycle management, and preparation of personalization data; or</td>
</tr>
<tr>
<td></td>
<td>• Manage associated cryptographic keys.</td>
</tr>
<tr>
<td></td>
<td>• The 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.</td>
</tr>
<tr>
<td></td>
<td>• 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;</td>
</tr>
<tr>
<td></td>
<td>• Card Manufacturing, Chip embedding, Personalization, Storage, Packaging, Mailing, Shipping or delivery, Fulfillment</td>
</tr>
</tbody>
</table>

NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Regulations</th>
<th>Payment Network Rules (e.g. Visa, MasterCard, American Express, Discover Network, ICB and debit card networks)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Regulation E: Electronic Fund Transfer Act (only for Signature debit transactions, N/A for credit card)</td>
</tr>
<tr>
<td></td>
<td>• Protects consumers engaging in electronic fund transfers (EFTs) and remittance transfers including: transfers through automated teller machine (ATMs) and point-of-sale (POS) terminals</td>
</tr>
<tr>
<td></td>
<td>• Covers initial disclosures</td>
</tr>
<tr>
<td></td>
<td>• Covers receipts and periodic statements</td>
</tr>
<tr>
<td></td>
<td>• Covers consumer liability for unauthorized transfers and error resolution</td>
</tr>
<tr>
<td></td>
<td>• Consumer has specific timeframes to limit liability or could become 100% liable</td>
</tr>
<tr>
<td></td>
<td>• Reg. 2 Truth In Lending &amp; Card Act for credit card transactions, but they do not address security</td>
</tr>
<tr>
<td></td>
<td>• NFC standards and protocols have been in existence for several years in use for non-payment activity. Many are global based, managed by NFC Forum in addition to ISO. NFC Forum provides technical specifications, not specific to payment security. Focus for SPTF should be standards around the payment process/wallet that leverages the NFC protocol. NFC/Contactless technology and communication protocols should be outside of the scope of SPTF other than for merchant POS terminals that may still have old terminals, with one-way NFC, although some may be addressing with (security) tokens.</td>
</tr>
</tbody>
</table>

FINCen Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) compliance; Know Your Customer (KYC); Office of Foreign Asset Control (OFAC)

Customer Identification Program (CIP) 31 CFR

NFC Forum - [http://members.nfc-forum.org/specs/spec_list/](http://members.nfc-forum.org/specs/spec_list/)

Near Field Communication.org - [http://nearerfieldcommunication.org/payment-systems.html](http://nearerfieldcommunication.org/payment-systems.html)

<table>
<thead>
<tr>
<th>Gaps/Issues</th>
<th>Most of the contactless/NFC standards and guidelines are very technical and relate primarily to data protection and message formats, not payment identity management. There are no known rules or regulations specifically addressing secure payment identity management for contactless/NFC payments. The SPTF SAT and PIM work group may want to consider whether this is a gap in payment security standards that needs to be addressed.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security/standards for QR codes for payments (e.g., Starbucks or Walmart model)</td>
</tr>
<tr>
<td></td>
<td>Security/standards for Beacons</td>
</tr>
<tr>
<td></td>
<td>No standards around enrollment</td>
</tr>
<tr>
<td></td>
<td>Non-phone mobile devices (e.g., watches) need fuller vetting</td>
</tr>
</tbody>
</table>

© 2017 Federal Reserve Banks. Materials are not to be used without consent.