Mobile and Digital Wallet Webinar Series
Part 2: Security Technologies & Approaches

January 23, 2019

U.S. Payments Forum Mission

- *… the cross-industry body focused on supporting the **introduction and implementation of EMV and other new and emerging technologies** that protect the security of, and enhance opportunities for payment transactions within the U.S.*

Current EMV-related Topics and Issues

- Petro, Transit and Hospitality merchants EMV-enablement issues
- EMV contactless/mobile acceptance testing & certification
- Issuer considerations for contactless EMV (dual interface, offline data authentication)

Beyond EMV – Advanced Payments Topics and Issues

- Mobile payment and tokenization
- Authentication: biometrics, future of CVM, new signature requirements
- 3-D Secure 2.0, Secure Remote Commerce and other CNP fraud tools

US PAYMENTS FORUM

Forum Activities & Resources

- **Collaboration on projects to develop resources to assist with U.S. EMV migration and implementation of other new and emerging payments technologies**
  - White papers, educational resources
  - Best practices and technical recommendations
- **Education programs for members and the industry**
  - Webinars, workshops, Forum member meeting tutorials, published resources
- **Communications**
  - Market outreach with recommended best practices and industry positions
- **Networking**
  - Forum for industry stakeholders to interact with all payments industry stakeholders

Information and resources available at www.uspaymentsforum.org

US PAYMENTS FORUM

Mobile & Digital Wallet Webinar Series

- **#1 – Mobile Wallet Landscape, Wallet Models and Processes – Jan. 9th**
  Review of five commercially-available wallet models with technologies and processes used in their implementation
- **#2 – Mobile Wallet Security Technologies and Approaches – Jan. 23rd**
  Review of different security technologies implemented in wallets
- **#3 – Strategic Considerations for Merchants – Feb. 6th**
  Review of key strategic considerations for merchants implementing a mobile wallet strategy
- **#4 – Strategic Considerations for Financial Institutions – Feb. 20th**
  Review key strategic considerations for financial institutions implementing mobile wallets

US PAYMENTS FORUM

Today's Speakers

- Randy Vanderhoof, U.S. Payments Forum

- Marianne Crowe, Federal Reserve Bank of Boston

Making the Mobile Wallet Secure

Lunch and Learn Education Series

Marianne Crowe
Vice President, Payment Strategies
Federal Reserve Bank of Boston
January 23, 2019

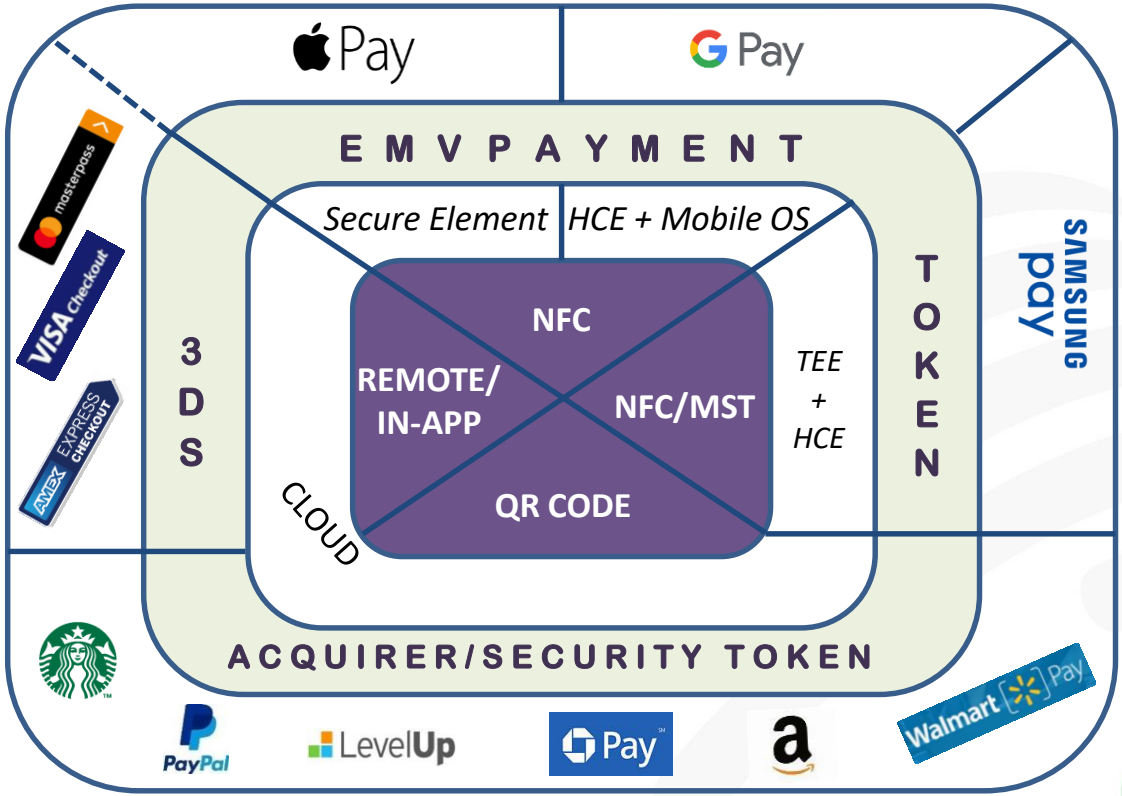
Agenda

- Overview
- Security of wallet models
  - NFC 'Pay'
  - Digital
  - QR Code
- Summary

Polling Question

- **Do you think mobile wallet payments are as secure as chip cards?**
  - **As secure** as chip cards
  - **More secure** than chip cards
  - **Less secure** than chip cards

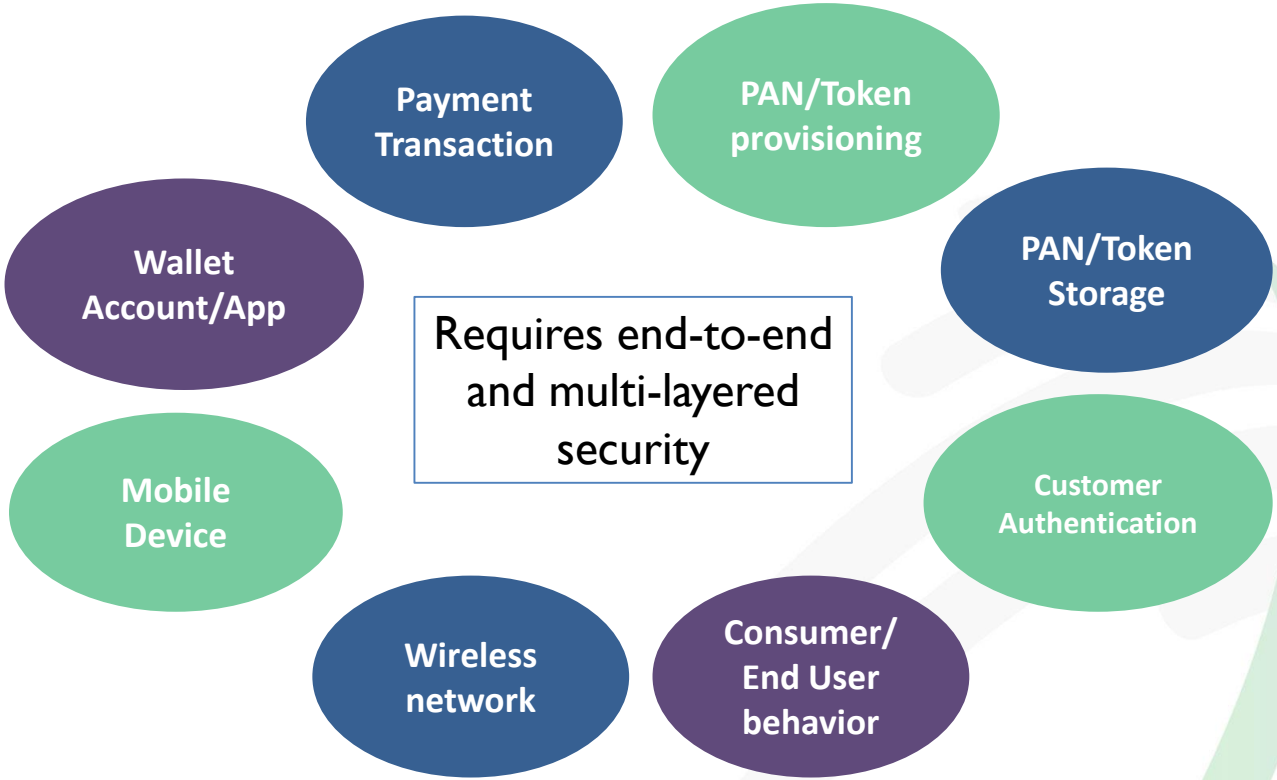
Wallets develop around key platforms



Source: Payment Strategies, Federal Reserve Bank of Boston, 2018

US PAYMENTS FORUM

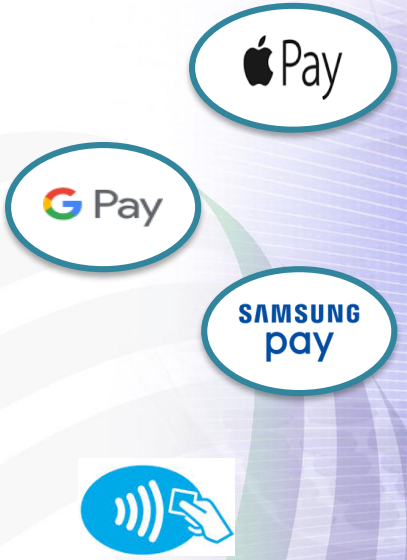
Wallets have multiple points of vulnerability



US PAYMENTS FORUM

POS ‘Pay’ wallets leverage common security methods

- EMVCo payment tokenization
  - Payment token replaces account number/ credentials (PAN) during transaction
  - Token is not mathematically related to the PAN
- Identity verification (ID&V)
  - Performed during enrollment before issuer provisions token to wallet
- User authentication
  - Biometrics (fingerprint, face) or passcode
- NFC communication protocol
  - To enable secure proximity-based contactless payments between mobile device and POS terminal



US PAYMENTS FORUM

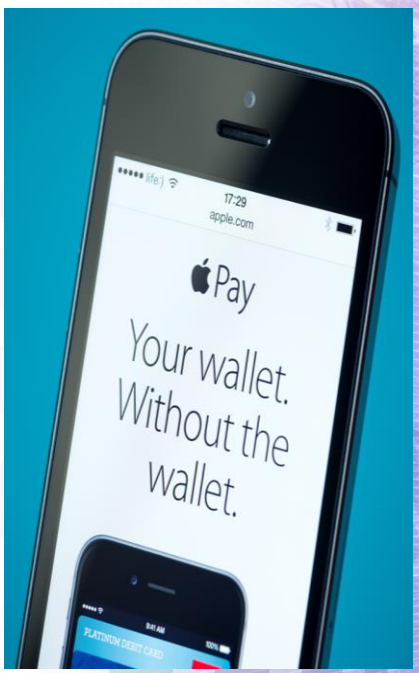
Payment tokenization follows highly secure structure

- Token Service Provider (TSP)
  - Generates and provisions payment token to customer mobile wallet
  - Manages secure centralized token vault containing actual PANs and associated tokens on behalf of issuer
  - Detokenizes (maps token to original PAN) and manages token life cycle
- Token Requestor (TR)
  - Authorized entity that requests/maintains tokens managed by TSP
  - Mobile wallet provider, merchant, card-on-file system, etc.
- High bar to become EMVCo TSP in U.S.
  - Payment networks are primary TSPs
  - 3rd party TSPs to date are TCH, First Data, PayPal
  - New TSPs must be registered by EMVCo and approved and certified by payment networks

US PAYMENTS FORUM

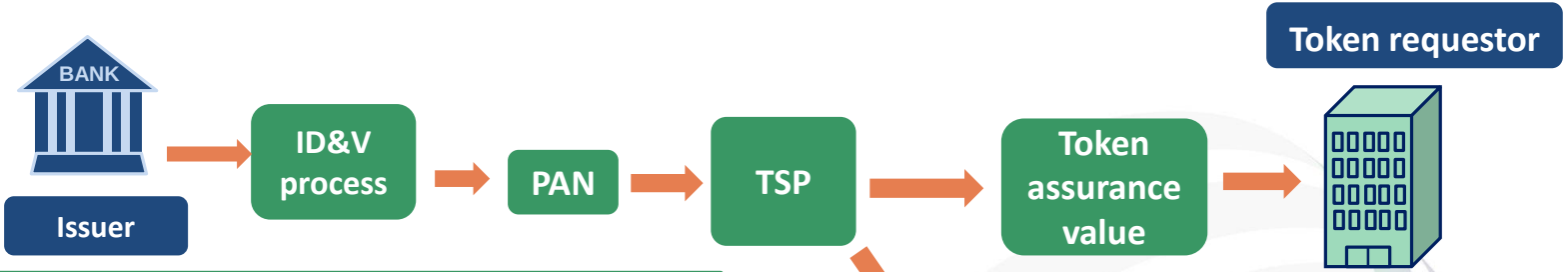
How EMV and payment tokenization secure credentials

- *Domain restrictions* limit use of token to channel, merchant, dollar amount, location, etc.
- Token only converted to PAN between TSP and issuer for authorization
- Dynamic data value (cryptogram) generated from data in contactless form factor and reader; dynamic transaction data is signed using a cryptographic key in the mobile phone during a transaction.
  - Tokenized transaction uses a cryptogram which is valid *only for one transaction*
  - Cryptogram authenticates transaction when validated using keys associated with issuer



Securing credentials during customer wallet enrollment

Identity and Verification (ID&V) to provision token



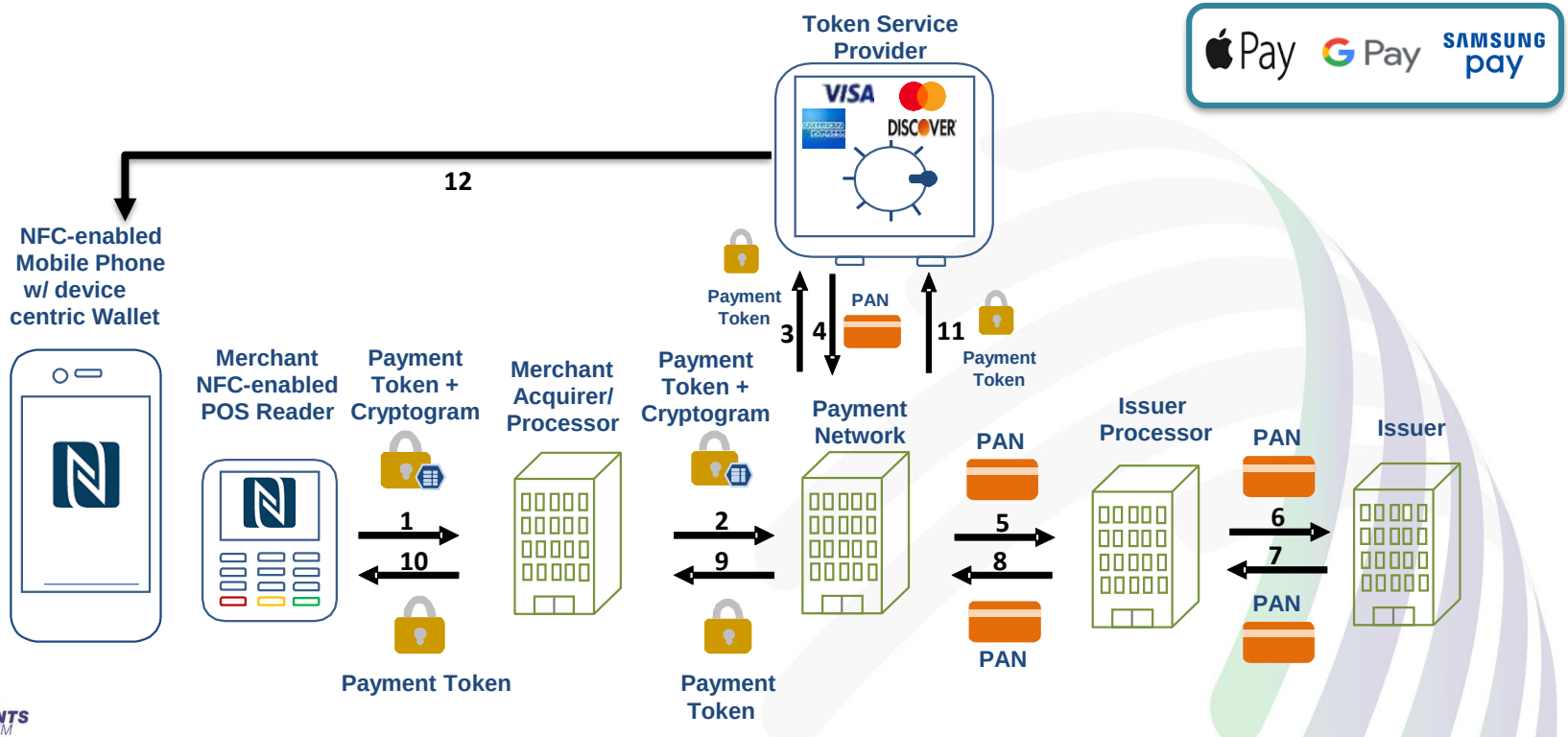
- Token requestor triggers ID&V with issuer
- Issuer validates cardholder/account (PAN) to establish confidence (i.e., token assurance level) for binding payment token to PAN/cardholder
- ID&V methods include: account verification message, risk score based on assessment of PAN, one-time password

TSP assigns value to token assurance level after issuer completes ID&V process

US PAYMENTS FORUM

Securing credentials during wallet transaction

Device-Centric POS Transaction Flow with contactless and payment tokenization



NFC enables payment tokenization for POS purchase

- NFC 'Pay' wallets reside on different mobile operating systems (iOS or Android)
- 'Pay' wallets store and retrieve payment tokens *differently*
  - *Apple:* *Secure element (SE)*
  - *Google:* *Host-card emulation (HCE)*
  - *Samsung:* *HCE for card emulation; Trusted Execution Environment/ (TEE) for secure storage*
- Other controls prevent downloading NFC wallet to rooted/jail-broken mobile phone

Apple Pay stores payment token in SE

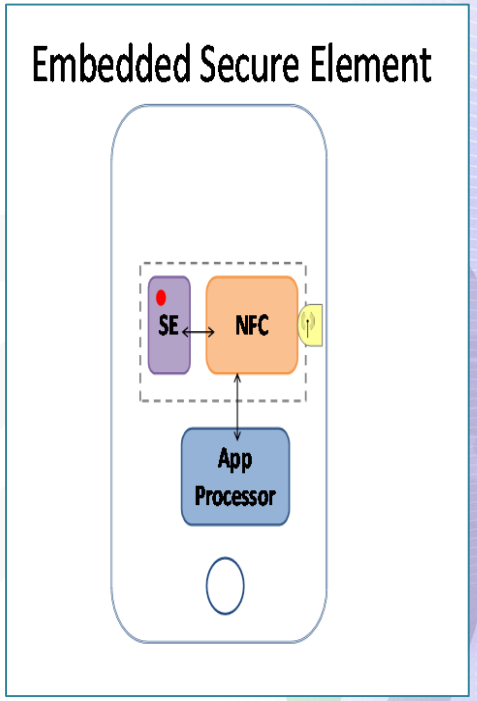
Secure element

- Tamper-resistant chip
- Embedded into mobile device during manufacturing, not removable
- Securely hosts applications and cryptographic data (e.g., wallet app, payment credentials or static token, cryptographic keys)

NFC controller

- Manages traffic and RF signals between mobile phone and POS terminal to pass token
- Built-in antenna communicates between mobile phone and POS terminal

Apple manufactures mobile device; controls access to SE



Google Pay uses Host Card Emulation (HCE) with NFC

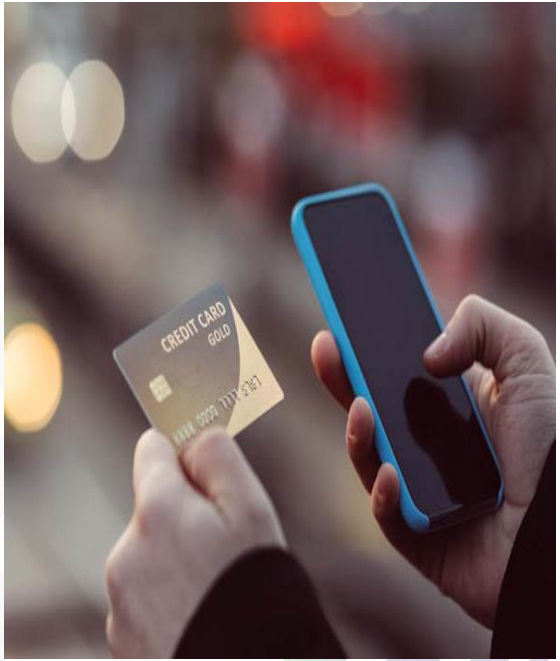
- HCE software emulates NFC card without physical secure element
- Master key representing PAN is stored in cloud
  - Generates dynamic token keys
  - Dynamic token keys downloaded and stored in secure area of mobile OS each time user connects to network
  - Storing dynamic token keys on mobile device enables transactions if no network connectivity
- POS terminal communicates with wallet to request dynamic token key for each transaction
  - Token key generates cryptogram passed with token to POS terminal
  - Dynamic token keys are restricted and expire quickly to minimize value to fraudsters
- Mobile OS considered less secure than SE
  - Requires additional software-based security (e.g., white box cryptography) to obfuscate the key

Samsung Pay stores payment credentials in TEE

- TEE embedded in secure area of main processor in mobile phone
  - Hardware and software with cryptography isolate and ensure secure storage and processing of sensitive data
  - Stores payment token and associated keys to generate dynamic cryptogram for each transaction
  - Protects trusted payment applications from other user-installed apps in mobile OS
  - Considered more secure than mobile OS, but less secure than SE because not tamper-resistant
- Samsung Pay MST (magnetic secure transmission) works without NFC but uses dynamic data/tokenization to enhance security

Using wallets in CNP channel creates new risks

- Volume of card-not-present (CNP) payments initiated via mobile (app or browser) is growing
- EMV chip migration shifted fraud from card-present to CNP transactions *(represented 61% of U.S. card fraud value in 2016, up from 48% in 2015)**
- Riskier because mobile device/owner not physically present, particularly if browser transaction
- Need enhanced tools to authenticate user and protect sensitive payment data/PAN but CNP security tools vary



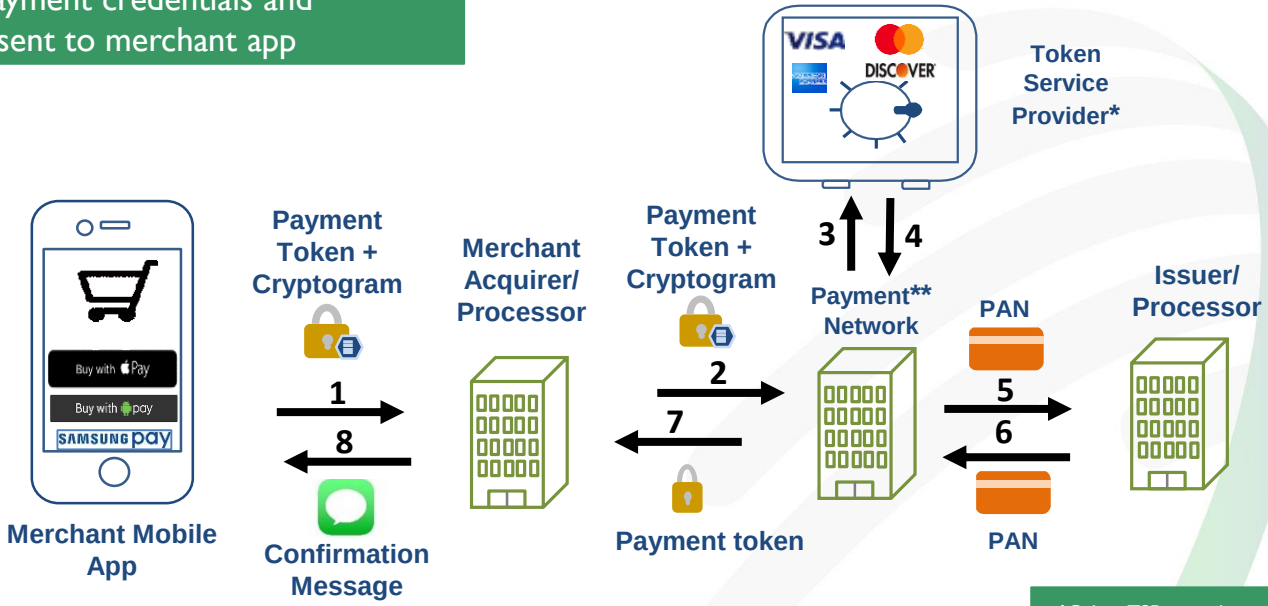
*https://www.federalreserve.gov/publications/files/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf

US PAYMENTS FORUM

“Pays” use common transaction flow for in-app transactions

In-App Device-Centric Wallet Transaction Flow with Tokenization on Merchant App

- Customer authorizes payment in merchant mobile app with biometric, PIN or passcode
- Tokenized payment credentials and cryptogram sent to merchant app

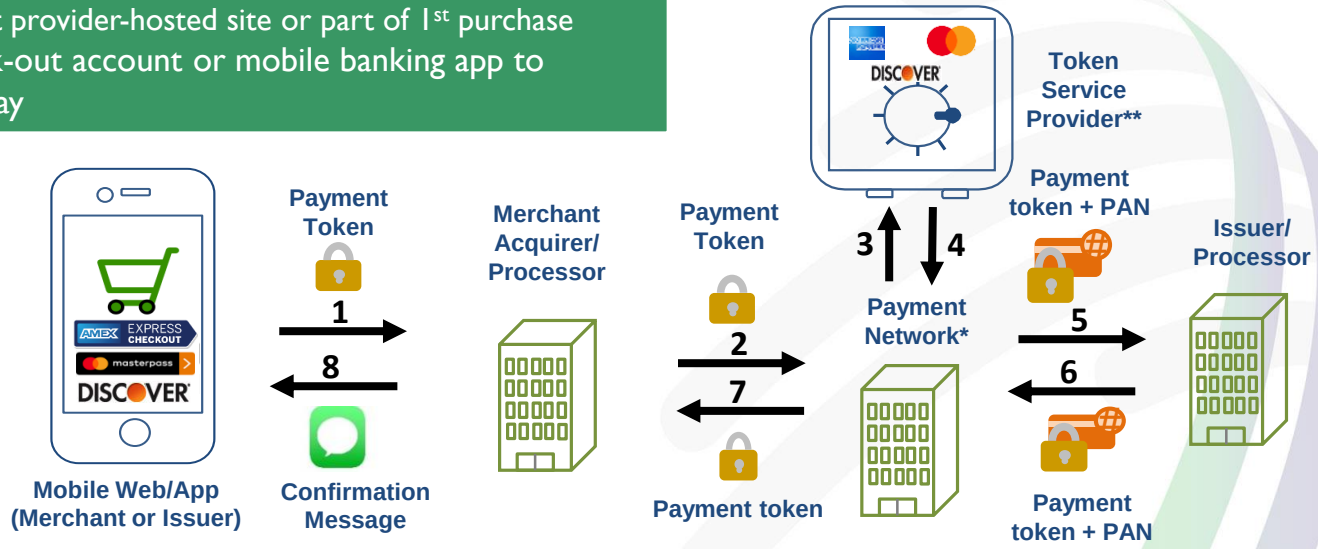


*Other TSP providers are also possible.
**Detokenization may not be possible by payment networks other than the card brand that owns the TSP.

US PAYMENTS FORUM

Payment network cloud-based digital checkout wallets simplify and secure customer buying experience

- Mastercard/Amex work directly or with FIs to tokenize cards in cloud wallet
- Any brand card can be added to cloud wallet (brand-agnostic) in some cases*
- Common enrollment options:
  - FI mobile app or online banking
  - Cloud wallet provider-hosted site or part of 1st purchase
- Login to check-out account or mobile banking app to authenticate/pay



* Payment network for in-app refers to token requested corresponding to card brand
**Detokenization may not be possible by payment networks other than card brand that owns TSP

“Cloud-based” digital wallets use proprietary tools

- Account takeover (ATO) fraud is one of largest growing attacks
  - Occurs at account creation where CNP accounts most vulnerable
  - User enrolls payment credentials and logs in with username/password – *most commonly stolen data*
  - Fraudster uses stolen login info to take over online accounts
- Large merchants and payment service providers (PSP) (e.g., PayPal, Amazon) use sophisticated risk engines and modeling tools to mitigate fraud related to ATO:
  - Perform behavioral analytics and transaction monitoring
  - Review customer profile data
  - Apply other authentication methods
  - Develop risk scores to accept or decline transactions
  - Tokenize Card-on-file (CoF) payment credentials

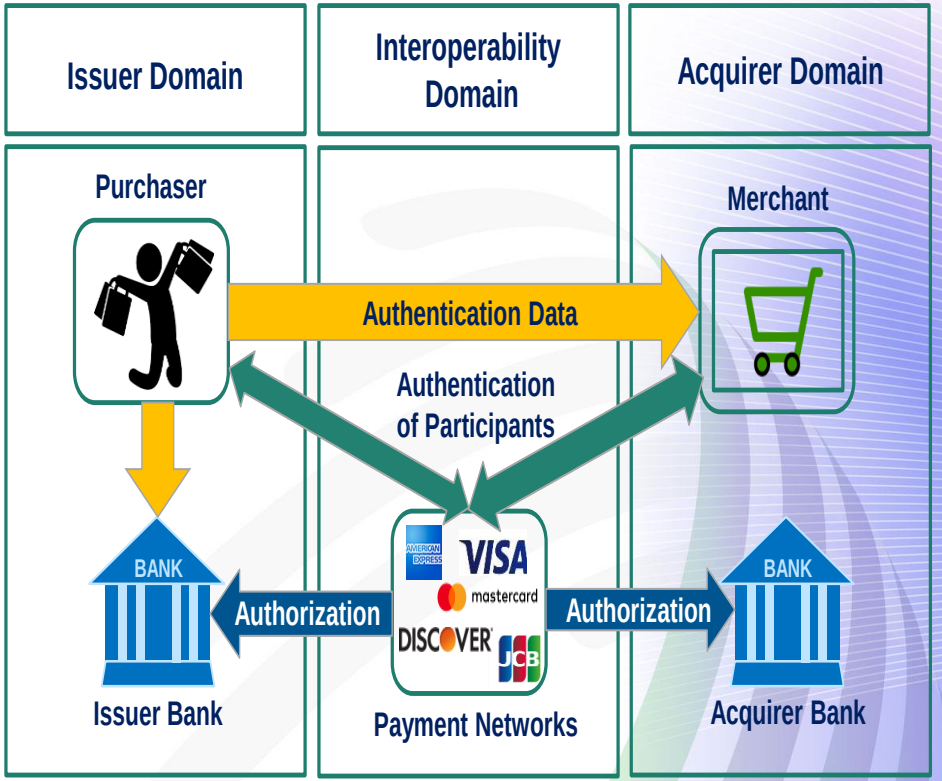
Risk-based authentication (RBA) enhances CNP security

EMVCo 3D-Secure (2.0)

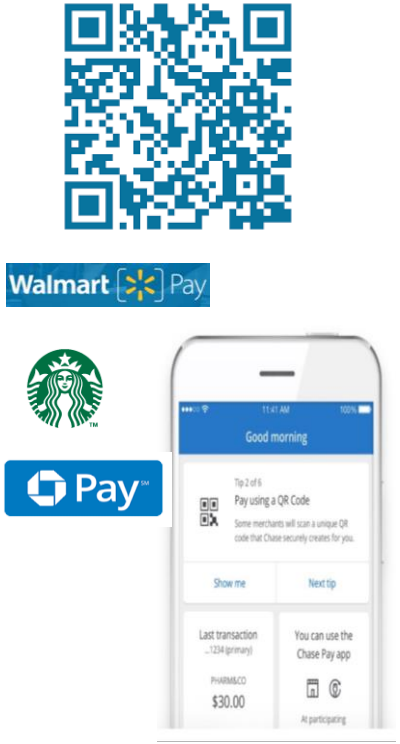
- Secure messaging authentication protocol that enables risk-based real-time cardholder authentication directly from card issuer during online transaction
- Liability for fraudulent transaction shifts to issuer when merchant uses 3DS
- Protects merchant from exposure to fraud-related chargebacks
- Improves online transaction security
- Encourages growth of ecommerce payments
- 3DS (1.0) developed before mobile payments
  - Knowledge-based authentication of all 3DS transactions
  - Customer friction and merchant frustration resulted in low U.S. adoption
  - EMV 3DS will replace 3DS 1.0 (2019)

EMV 3DS (2.0) more merchant/customer-friendly

- Risk-based decision process authenticates ONLY when risk exceeds predetermined level
  - Merchants and issuers exchange more data to determine risk (e.g., device ID, geo-location, phone #, email, address)
  - Issuer determines need for additional authentication on higher risk transaction but merchant can refuse
  - Additional authentication done on ~5% of transactions
- Participating issuer's customers are auto-enrolled
- Supports mobile browser/app, PC browser



QR (quick response) code wallet security

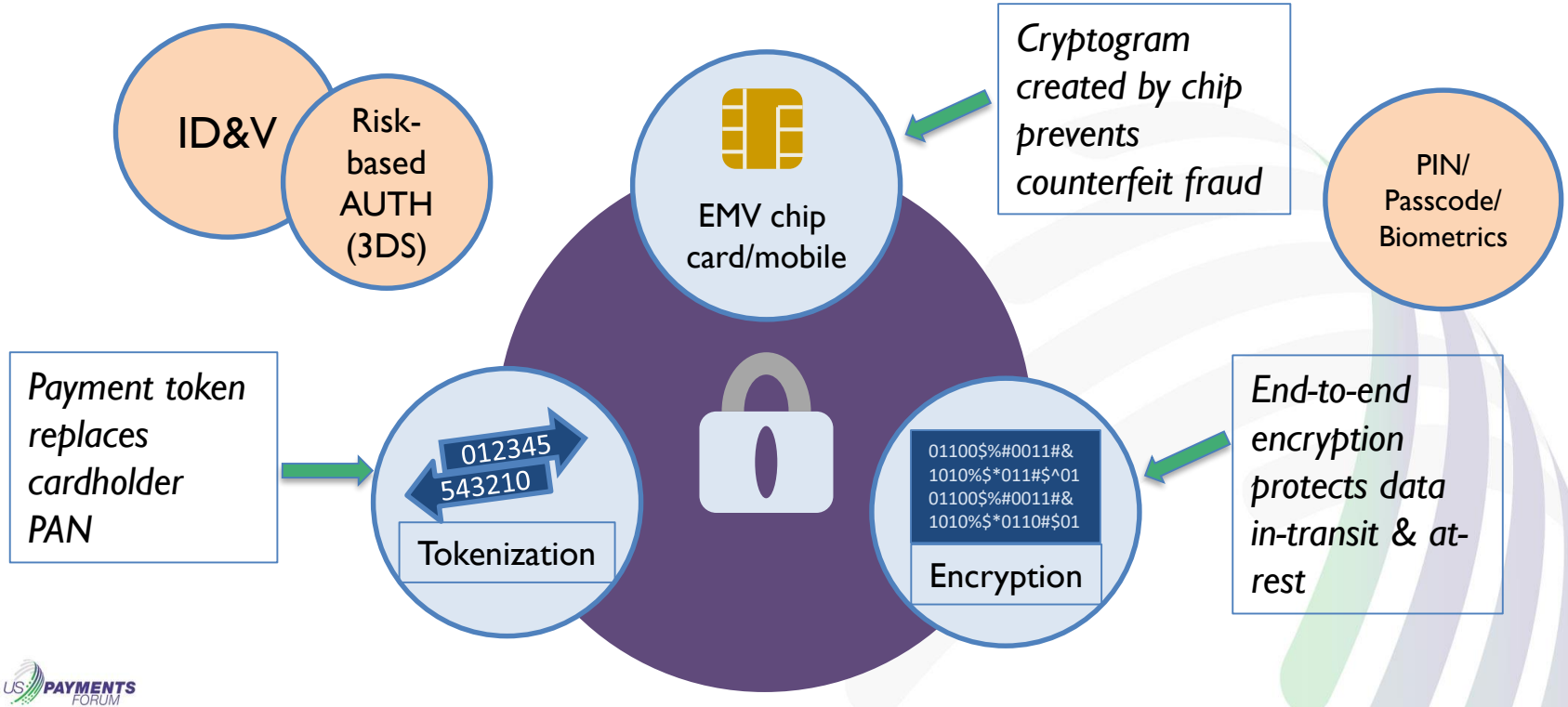


- QR code randomly generated to map to real PAN
- PAN stored in proprietary cloud/merchant server, NOT on phone
- Passcode/fingerprint screen lock prevents fraudulent access to device and phone camera
- PCI requires payment data to be encrypted during transmission and at-rest
- QR code wallet tokenization
  - Chase Pay generates unique payment token for each payment card enrolled in its wallet
  - Walmart Pay generates QR code 'token' to authorize payment without exposing PAN
- EMVCo introduced specs in 2017 to ensure consistency in QR codes generated or captured on consumer mobile phone
  - Two QR code models: merchant-presented and consumer-presented

US PAYMENTS FORUM

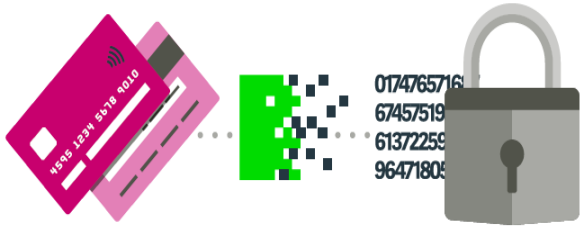
Multi-layered security options

No one method can protect each payment or all wallets



Summary of Key Points

- Mobile wallets leverage security provided by the mobile device, the hardware and software components in the mobile OS, and the mobile app
- If used appropriately, and both physical and logical components are protected, mobile wallets can effectively secure payments
- Broad use of effective, multi-layered security approaches for all wallet models is still lacking
- Increased awareness and education across stakeholders (issuers, merchants, processers and consumers) is key



Polling Question

- **Now that you have heard the presentation, do you think mobile wallet payments are as secure as chip cards?**
  - **As secure** as chip cards
  - **More secure** than chip cards
  - **Less secure** than chip cards

Q&A

US PAYMENTS FORUM

www.uspaymentsforum.org

Mobile Wallet Webinar Series: Online Assessment

- Online assessment quiz available for each webinar in the series
- Participate in all four webinars and assessments to receive a certificate and registration discount to the 2019 Payments Summit
- Assessment link: https://www.surveymonkey.com/r/walletwebinar2

US PAYMENTS FORUM

Additional Resources

- **March U.S. Payments Forum Member Meeting and 2019 Payments Summit**, Mar. 11-14, Phoenix, AZ
  - **Mar. 11-13 – Forum Member Meeting**: roundtables, SIGs, working committee and birds-of-a-feather sessions
  - **Mar. 12-14 – 2019 Payments Summit**: multiple tracks covering all things payments, including FinTech, EMV chip technology, mobile wallets, NFC, contactless, open transit systems and more
- **Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions** white paper, http://www.uspaymentsforum.org/mobile-and-digital-wallets-u-s-landscape-and-strategic-considerations-for-merchants-and-financial-institutions/
- Other resources available at: www.uspaymentsforum.org

Randy Vanderhoof, rvanderhoof@uspaymentsforum.org
Marianne Crowe, Marianne.Crowe@bos.frb.org

US PAYMENTS FORUM

www.uspaymentsforum.org