Tokens, Tokens, Tokens: What are the different kinds of tokens and what do they do?

Lanny Byers, VP
Emerging Payment Solutions

February 25, 2019/3:30PM/Grand Ballroom J-K
The way consumers buy has changed for good
Commerce access is expanding globally

Any Device – Anywhere, anytime

<table>
<thead>
<tr>
<th>Computers</th>
<th>Mobile</th>
<th>Internet of Things (IoT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>via web browsers</td>
<td>via web browsers or apps</td>
<td>Diverse range of devices (e.g., cars, wearables, gaming consoles, vending machines) that use embedded technology to communicate and interact with the external environment via the Internet</td>
</tr>
<tr>
<td>• Desktops</td>
<td>• Smartphones</td>
<td></td>
</tr>
<tr>
<td>• Laptops</td>
<td>• Tablets</td>
<td></td>
</tr>
</tbody>
</table>

Societal transformation
Behaviors and Impacts are Changing Rapidly
User numbers are huge

3.2B Internet
2.5B Messaging
2.0B Social Media
Consumers want fast, frictionless payments
Merchants want consistent, frictionless experiences for consumer in any channel with:

- Data and analytics
- Security and fraud
- Payment type, device and routing choice
- Global commerce
- Loyalty, rewards, and private label cards
Consumers want...any payment type, anywhere and the merchant knows me...

Frictionless shopping experiences for a connected world

Any channel

Enabling payment on any device

With any payment method

Securely and at scale

<table>
<thead>
<tr>
<th>Web/Online</th>
<th>Recurring pay</th>
<th>Brick-and-mortar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web/Online</td>
<td>Recurring pay</td>
<td>Brick-and-mortar</td>
</tr>
</tbody>
</table>

Any channel

Enabling payment on any device

With any payment method

Securely and at scale

2019 MID-YEAR CONFERENCE  February 25-27 | Ft. Lauderdale, FL
Frictionless digital shopping experiences securely and at scale require tokenization

- Loyalty and offers
- Line busting/Order customization
- Pick up and delivery
- Car ordering and payments
- Pay at the pump
- Pay at table
Tokenization is the key digital pay ingredient

New infrastructure starts with tokenization
- New open payment systems all rely on tokenization
- EMVCo tokenization is required for debit and credit payment transactions to flow thru payment networks
- Non-EMV tokenization can be leveraged for proprietary wallets, apps, and card-on-file scenarios; as well in-store transactions

Tokenization is challenging
- Equipment vendors and scheme operators will face hurdles on how to make multiple technologies work together
- Any solution needs to be flexible in adding new payment methods that will be driven by the consumer and how they wish to accept funds and pay

New payment types will require new tokenization specs
- As faster payments evolve as a potential new payment type, tokenization specs will be required
- New reader certification may be required
Card tokenization

Securing the Primary Account Number (PAN)

EMVCo Tokenization replaces a card’s PAN with a number unique to a specific device, merchant, transaction type, or channel.

What does a card token do?
Improve security by eliminating the risk of exposing PAN data within systems/files or transactions.
Components of token service

**Provisioning**
- Validates card data as requested by TSP
- Offers issuer-defined data elements

**Authorization**
- Receives and forwards token and PAN data
- Stores token info related to digital payment transactions

**Maintenance**
- Provides interface/enables maintenance on tokens via customer service portals

**Value added services**
- Loyalty programs
- Instant digital issuance
- Additional possibilities

**Reporting**
- Provides reporting to issuer on token activity
Token Service Providers

Life Cycle Management by the TSP enables the issuer to activate, resume, suspend or delete the token

- Expired Card
- Lost/Stolen Card
- Lost/Stolen Device
- Reissue PAN or Expire Date
- Update
- Suspend/Deactivate
- Reactivate
- Cancel

Token Service Providers

- **First Data** - Universal Token Services (FDUTS)
- **Mastercard®** – Digital Enablement Services (MDES)
- **Visa®** – Visa Token Services (VTS)
- **American Express®** – Token Service
- **Discover®** – Digital Exchange (DDX)
- **The Clearing House®** – Secure Token Exchange
Card tokenization

Use cases and future vision

The following slides will show various use cases of how tokenization works today.

How do EMV® tokens get requested and used by Pay Wallets?

How do Non-EMV tokens get requested and used by merchants?

How do EMV tokens get requested and used by Card-On-File merchants?

Merchants lose track of the customer.
Pay wallet requests EMV token

**Consumers** enroll with pay wallet and registers their PAN and other payment data.

**Merchants** have no interaction in this initial process and requires merchants to accept NFC at point-of-sale and in-app.

Token vaults are maintained by token service providers which can be payment networks, payment processors or others.

Token and cryptogram sent to the acquirer and token and cryptogram are sent to TSP for detokenization and crypto validation.
**Pay wallet in-store NFC transaction**

**Consumer** uses Pay Wallet (Apple Pay, Google Pay, etc.) at contact-less point-of-sale.

**Merchant** sends token to acquirer processor and token is routed to TSP to de-tokenize and send PAN to Issuer for authorization. Token returned to acquirer processor and on to merchant.
**Pay wallet in-app transaction**

**Consumer** makes purchase with Pay Wallet (in-app) which is the EMV token and is not registered with merchant.

**Merchant** sends token to acquirer processor and EMV token is routed to TSP to de-tokenize and send PAN to Issuer for authorization. EMV token returned to merchant. In this scenario customer is invisible unless they have registered with merchant.
In-store card transaction, results in non-EMV token

Consumer makes in-store purchase with plastic card at merchant that uses a merchant token vault.

Merchant sends PAN to acquirer. Acquirer sends PAN to issuer for authorization. PAN is converted into a non-EMV token and returned to merchant.
Card-on-file merchant requests non-EMV token

Consumers want choice of device and channel to shop – via mobile device or web. They expect it to be frictionless and the same. Consumer registering with merchants web site and places card-on-file.

Acquirer processor handles the request and stores the PAN and creates a non-EMV token – returning a non-EMV token to the merchant. Non-EMV tokens can be used for proprietary wallets/apps.

Token vaults are maintained by token service providers which can be payment networks, payment processors or others.
Card-on-file merchant transacts with non-EMV token

**Consumer** makes purchase on-line and checks out using existing on-line account and enrolled PAN with merchant (non-EMV token on file).

**Merchant** sends token to acquirer processor and transaction/PAN routed to issuer for authorization. PAN and authorization returned to acquirer processor and on to merchant as a non-EMV token.
In-store QR transaction with non-EMV token

**Consumers** makes purchase with merchant app and is registered with merchant (non-EMV token) with card-on-file.

**Merchant** sends non-EMV token to acquirer. Acquirer will de-tokenize token and send PAN to issuer for authorization. PAN is converted into a non-EMV token (back into existing token) and returned to merchant.

**Issuer**
Card-on-file merchant requests EMV token

Merchants may want to use EMV tokens for card-on-file. Consumer registering with merchants web site and places card-on-file. Work with EMV Token Vault provider.

EMV token vault handles the request and stores the PAN and creates an EMV token – returning an EMV token to the merchant. Non-EMV tokens not available.
**Card-on-file merchant transacts with EMV token**

**Consumer** makes purchase on-line and checks out using existing on-line account and enrolled PAN with merchant (EMV token on file).

**Merchant** sends token to acquirer processor and token is routed to EMV token vault to de-tokenize and send PAN to issuer for authorization. Token returned to acquirer processor and on to merchant.
Merchants lose track of the customer

Merchant gets back multiple tokens for the same PAN...same customer... depending on which device, wallet, and channel the customer used to transact with the merchant.

This issue needs to be resolved in order to provide the customer with the best shopping experience.