Smart Card Alliance

EMV Tokenization

November 3, 2016

Smart Card Alliance

Smart Card Alliance Mission

To stimulate the understanding, adoption, use and widespread application of smart card technology through educational programs, market analysis, advocacy, and industry relations . . . .

Mobile Council

Building industry awareness around the business and security impacts of utilizing different technologies for distributing, storing and using secure credentials on personal mobile and tethered wearable devices.

Recent Mobile Council Resources

- *EMV and NFC: Complementary Technologies Enabling Secure Contactless Payments*
- *Host Card Emulation: An Emerging Architecture for NFC Applications Webinar*

Today's Webinar Topics and Speakers

- **Introductions**
  - Randy Vanderhoof, Smart Card Alliance
- **Introduction & Tokenization Overview**
  - Sadiq Mohammed, MasterCard
- **Implementation Considerations for Tokenization**
  - Sree Swaminathan, First Data
- **Security Considerations for Tokenization**
  - John Sheets, Visa
- **Summary & Conclusions**
  - Randy Vanderhoof, Smart Card Alliance
- **Q&A**
  - Randy Vanderhoof, Smart Card Alliance

Introduction & Tokenization Overview

Sadiq Mohammed, MasterCard

What Is Tokenization?

Tokenization [tō ˈkən əˈzā shən]

Tokenization *is the process of substituting a sensitive data element with a unique non-sensitive equivalent, referred to as a* ***token****, that has no extrinsic or exploitable* ***meaning*** *or* ***value****.*

Token values vary in format and may be cryptographically or non-cryptographically generated – varies by type of token, use case and solution

Tokens are generated, stored, mapped/de-mapped within a secure centralized system called a ***Token Vault****.*

Detokenization *is the process of mapping the token back to its original value*

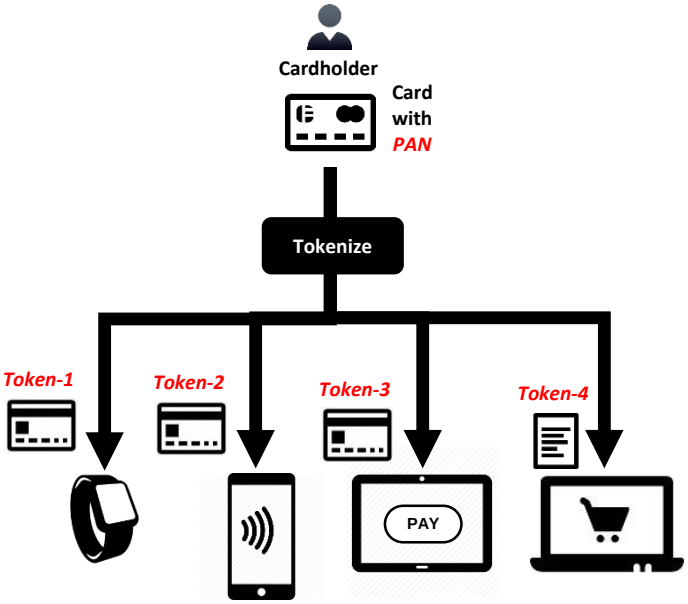
An entity providing Tokenization/Detokenization is typically referred to as a ***Token Service Provider***

Where Does Tokenization Play a Role in Payments?

Tokenization is used to replace a consumer card's Primary Account Number (PAN) with an alternative value called a Token, in order to protect the consumers account information

Token Features:

- A single PAN may be mapped to multiple tokens for different use cases
- Tokens may be merchant, channel or device specific and single or multi-use
- If compromised or stolen, tokens reduce the likelihood of subsequent fraud since they have no value outside a specific device, merchant or acceptance channel



What Are the Different Types of Payment Tokens?

Characteristics	Payment Token Type		
	Acquirer Token	**Issuer Token**	**EMV Token**
Token Purpose	• Created within the closed environment of the merchant and acquirer and used to remove sensitive account data from the merchant environment	• Created by the issuer to tie multiple PANs to the same user account. Some of these PANs may be temporary or for one time use while some may be to enable a sticker or card accessory.	• Created by token service provider on behalf of the token requestor to substitute for a PAN during the entire transaction process. These tokens are typically specific to a particular device, transaction type or merchant.
Token Format	• Alpha-numeric or numeric characters of acquirer-desired length/type	• PAN-formatted number issued under an issuer BIN / card range	• PAN-formatted replacement value based on a designated Token BIN or Token Card Range
Token Provider	• Acquirer, Processor, Payment Services Provider, Gateway	• Issuer or Issuer Processor / Agent	• Payment Network or Issuer/Issuer Processor or EMVCo enrolled TSP.
Transparency	• Merchant to Acquirer only	• Issuer only	• Transparent to all participants
Usage Restrictions	• Usage restricted to controlled payment interactions between a given merchant and token service provider	• May have limits on its usage (frequency, amount, domain) by the issuer and its vault	• Offers usage restrictions to given token requestors and domain(s) to minimize fraud impacts if data is exposed

What Is Special About an EMV Payment Token?

EMV Payment Tokens look exactly like a regular PAN, pass through the payment system without any changes, but are processed differently and may have domain restrictions to protect them from improper usage.

EMV Payment Tokens will:

- Not 'collide', or conflict, with an actual card issuer assigned PAN
- Pass basic validation rules of an account number, while reinforcing interoperability
- Be mapped and associated with an underlying PAN by the entity that generates it, and issues it to the requestor
- Be accepted, processed and routed by the entities within the ecosystem (merchants, acquirers, payment processors, payment networks, card issuers)
- Be a 13 to 19 digit numerical value that conforms to the account number rules of an ISO message ('like-to-like' formatting)

Smart Card Alliance

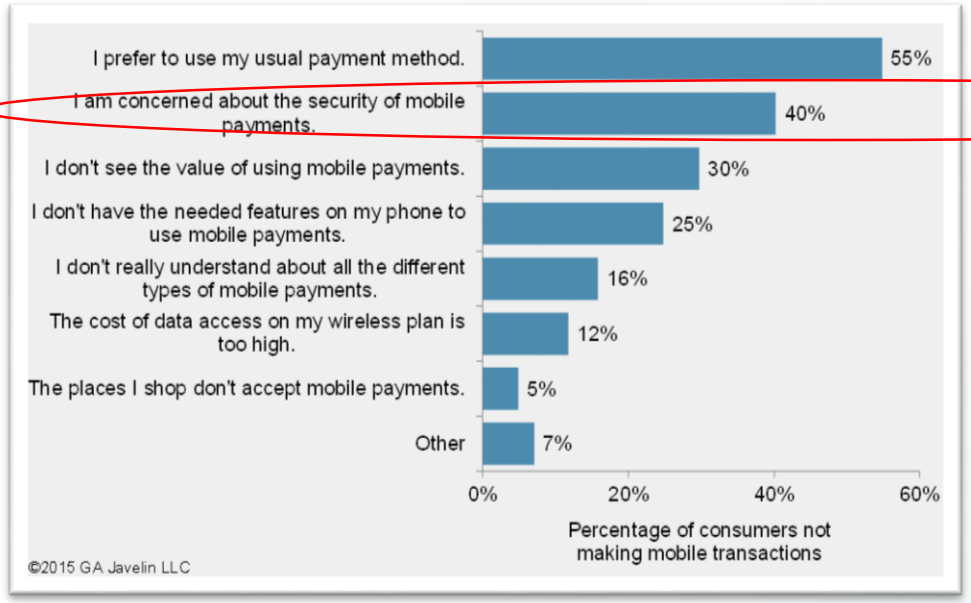
How Does EMV Tokenization Help?

An interoperable standards based approach will help enable adoption and facilitate newer models in the existing payment eco-system…

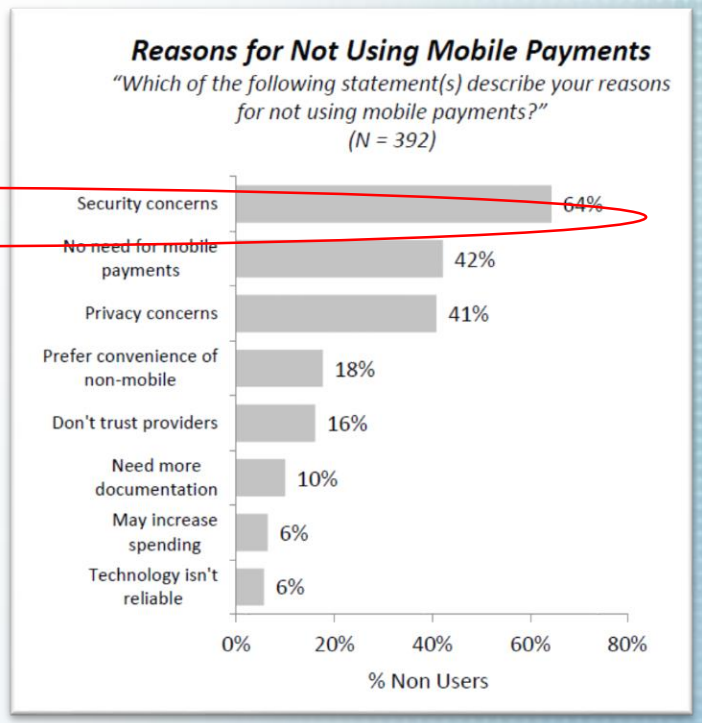
Smart Card Alliance

Why Has Tokenization Gained Importance?

- Increasing security on mobile devices is a key driver
- Proliferation of devices increases risks with a single PAN
- Card reissuance and updates have become a major pain point that is addressed by tokenization
- The need to support more paths for commerce in a controlled manner



Source: Javelin: The Evolution of Tokenization in a Mobile Payments Environment, Dec 2015



Source: First Annapolis: Study of Mobile Banking & Payments, Third Edition, August 2016

Where Can We See Tokenization in Action?

Major Device-based Wallets have all utilized Tokenization

Apple Pay

Android Pay

Samsung Pay

Microsoft Wallet

Major EMV Token Service Providers

Amex Token Service

Discover Digital Xchange

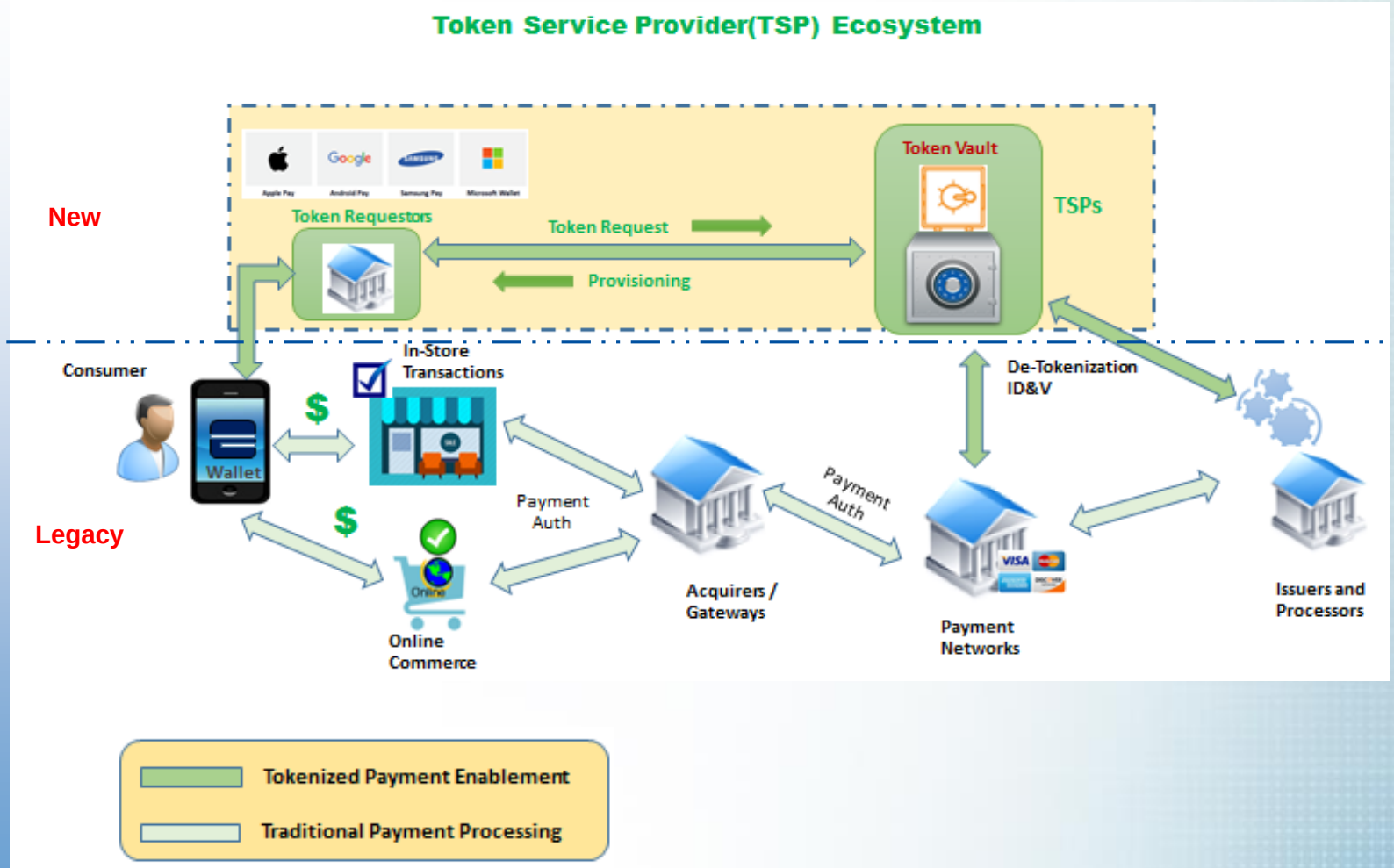
MasterCard Digital Enablement System (MDES)

Visa Token Service (VTS)

Implementation Considerations for Tokenization

Sree Swaminathan, First Data

Where Does a TSP Fit In the Payments Ecosystem?



What Is the Role of a Token Service Provider?

Key Concepts & Functions:

Token Generation/Issuance: The TSP is responsible for setting up PAN and Token ranges and generating tokens that does not collide with existing PANs and that are in accordance with EMVCo Tokenization standards.

Token Vault: The generated tokens and the original PANs they map to are stored securely in a token vault and the mapping is used during the detokenization process.

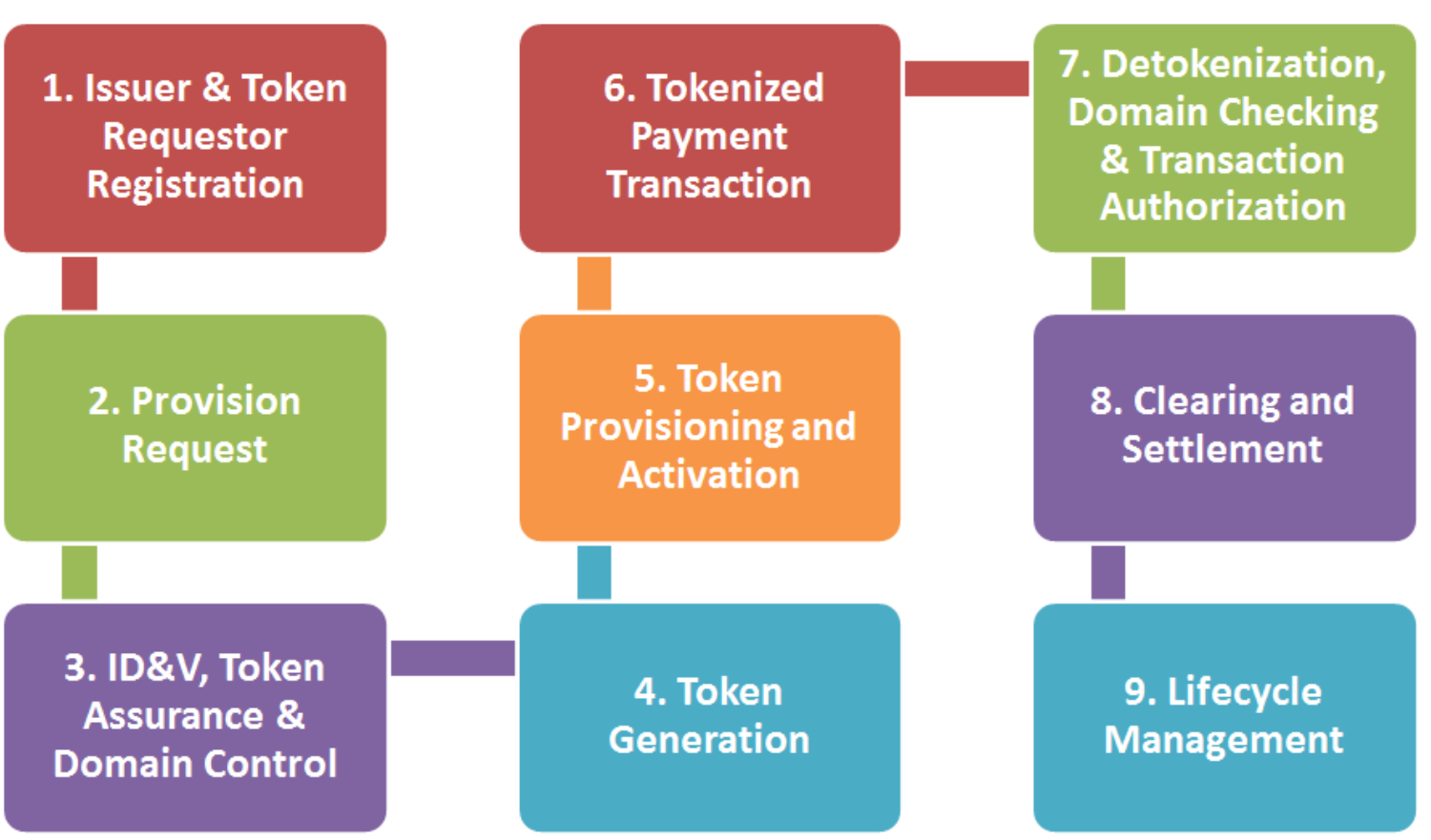
ID&V and Token Assurance: The TSP enables a Identification and Verification Process (e.g. KYC, CVC/AVS verification) to derive a risk score. Accordingly, a token may have an Assurance Value between 0-99 based on risk profile and strength of ID&V.

Token Domain Restriction: Assigning a token to a specific device, channel, merchant or geographic location or a combination of these to restrict the transaction within that domain.

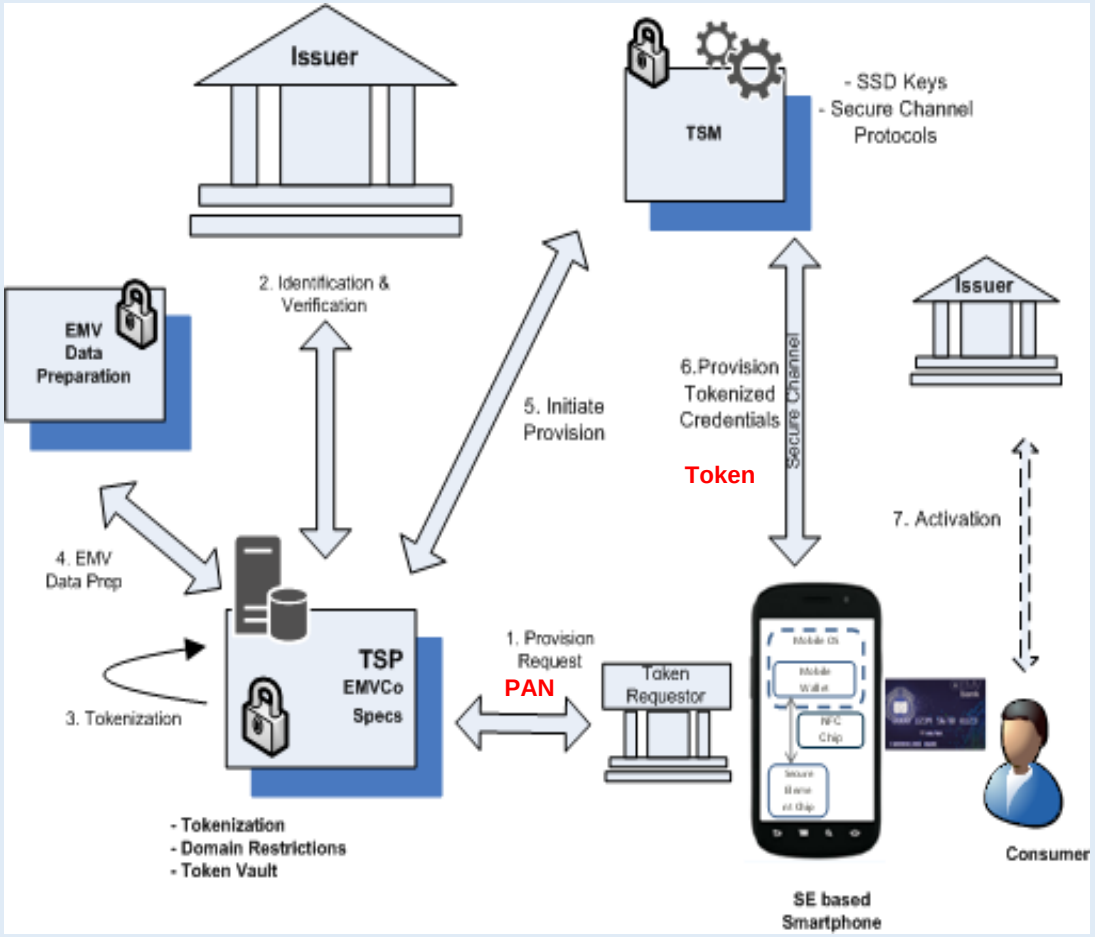
Token Lifecycle Management: The process of continually managing the token through suspension, deletions, updates, etc.

Smart Card Alliance

How Does a Token Come to Life and Get Used?

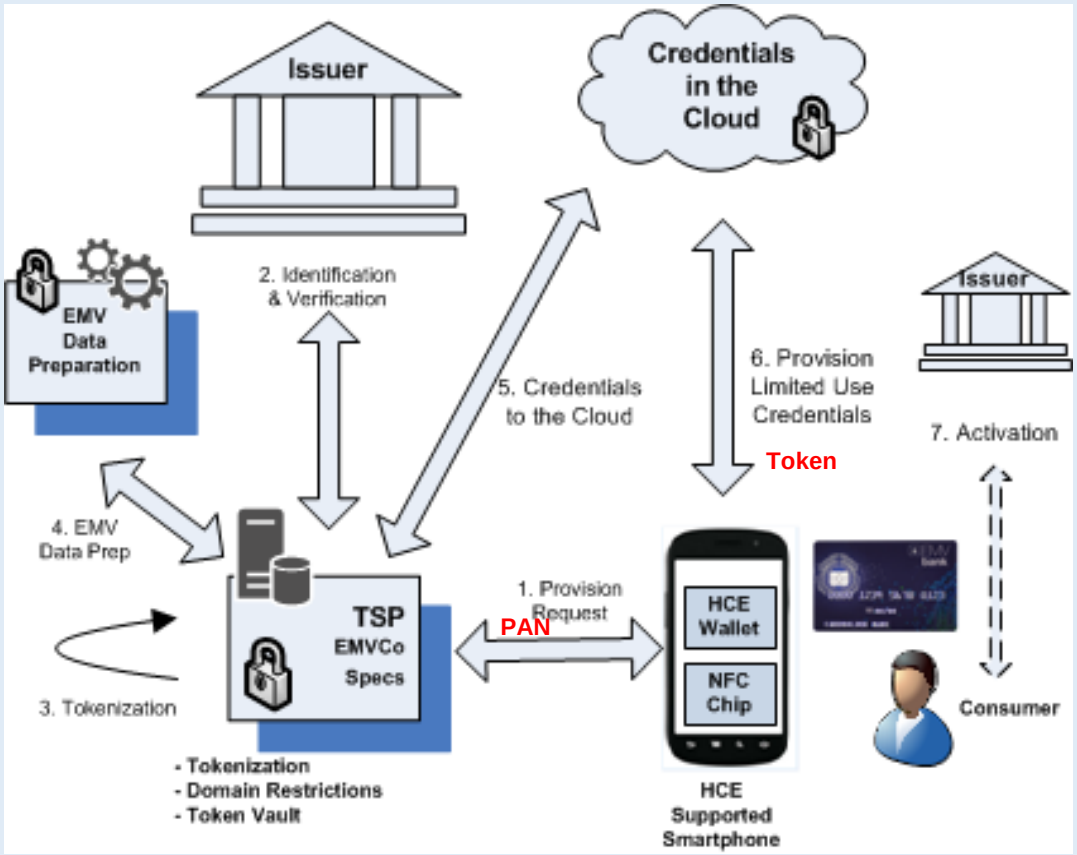


Detailed Token Provisioning Flow(SE)



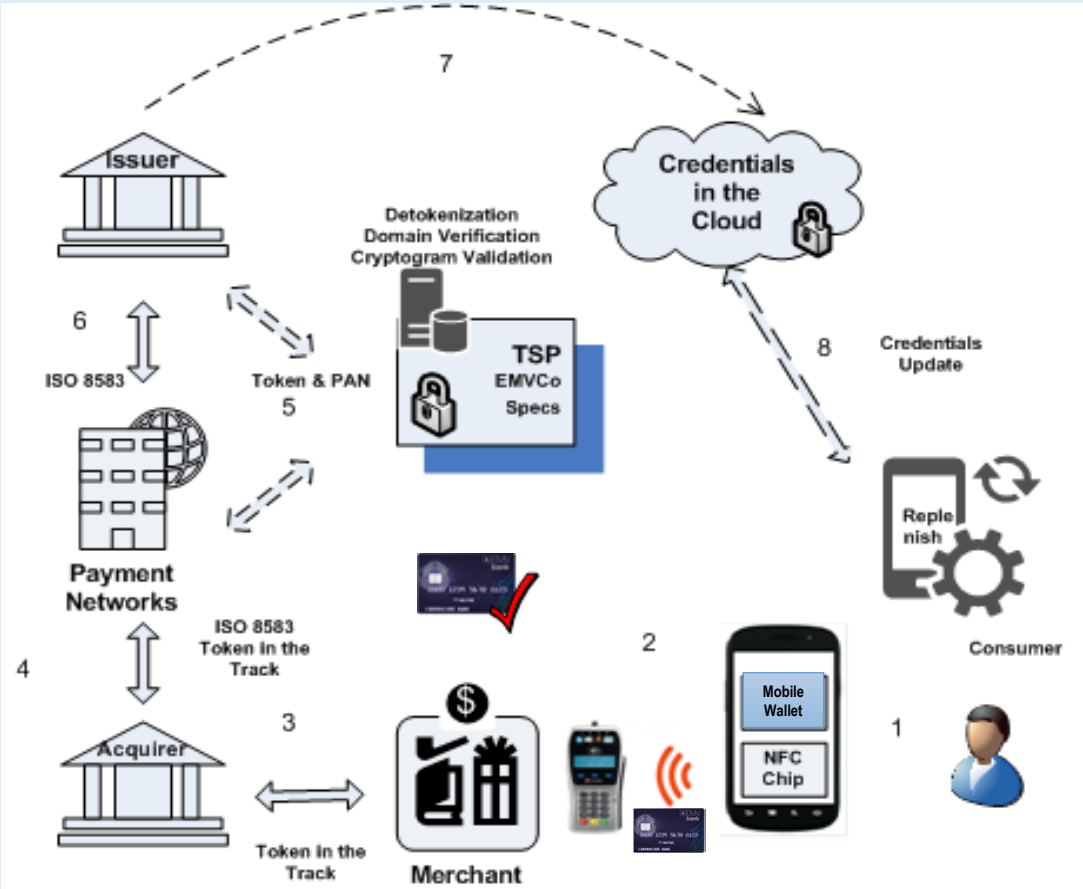
1. Enrollment/Provision Request
2. Identification and Verification
3. Tokenization
4. EMV Data Prep
5. Provision request to TSM
6. Provision Credentials to the Secure Element in the Device
7. Activation

Detailed Token Provisioning Flow(HCE)



1. Enrollment/Provision Request
2. Identification and Verification
3. Tokenization
4. EMV Data Prep
5. Provision Request to the Cloud
6. Provision Limited use Credentials to the Device
7. Activation

Token Use During an In-Store Transaction



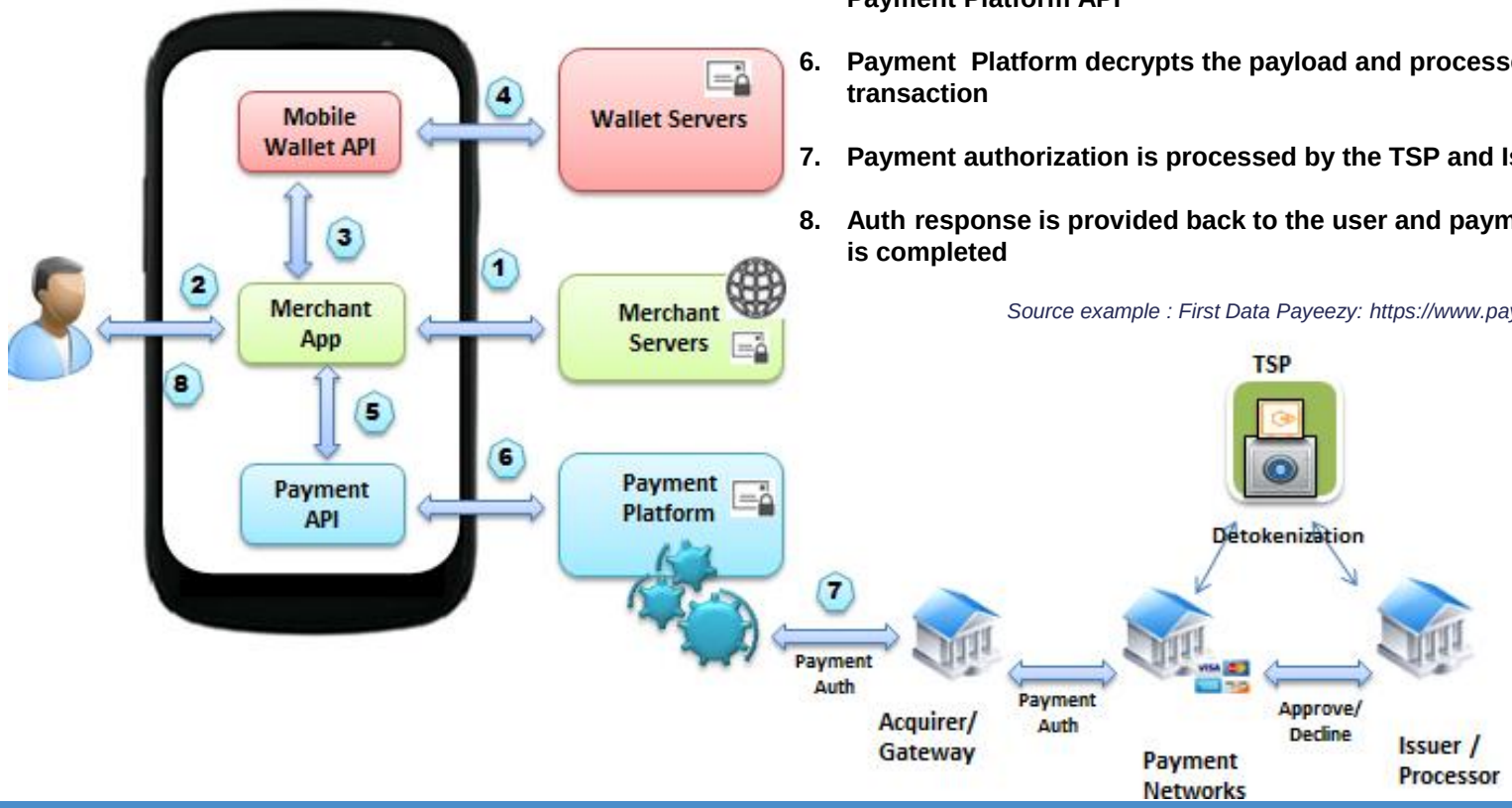
1. Initiate Payment
2. NFC Transaction
3. ISO Auth Message
4. Authorization Request/Response
5. Routing / Detokenization
6. Detokenization/Crypto Validation/Auth Response

7-8. Host Synchronization, Life Cycle Management, Credentials Update (HCE Use case)

Token Use During an In-App Transaction

1. **Merchant provides Buy options to the consumer for the merchandise**
2. **Consumer taps the Pay button to complete the transaction.**
3. **Payment request sent to Mobile Wallet App**
4. **Merchant App obtains the encrypted transaction payload back from Wallet API and servers**
5. **Merchant App sends the payload to Payment Platform using the Payment Platform API**
6. **Payment Platform decrypts the payload and processes the transaction**
7. **Payment authorization is processed by the TSP and Issuer**
8. **Auth response is provided back to the user and payment transaction is completed**

Source example : First Data Payeezy: https://www.payeezy.com



Token Life Cycle Management

Life Cycle events can be triggered by issuers, consumers, TSP, Token Requestors, Card Networks, etc.

Token Life Cycle Management is the process of continually managing the tokens from the time of creation to suspension, deletions, updates, etc.

Stakeholder Considerations for Tokenization

Issuers:

- Ensure Token Service Providers have necessary certifications and approvals
- Ensure TSPs have a secure interface and authenticate all TSP requests
- Understand the alignment with existing card programs
- Cardholder and employee education on tokenization
- ID&V decisioning and additional security such as step-up authentication

Acquirers/Processors:

- Tokenized transactions that require new fields and messages to be supported
- May require additional requirements to support cryptograms and dynamic data
- Enable new payment channels and domains

Merchants:

- Ensure POS supports NFC transactions
- Consider Wallet provider, Network guidelines for Token transactions
- Potential impact to loyalty programs as some consumers may transact with different tokens
- Loyalty, Marketing and Promotions impact to existing programs in place(PAR field may have to be considered)
- Understand returns in Tokenized transactions

TSPs :

- Enable Issuers and Token Requestors to request Tokens for multiple channels and domains (NFC –SE/HCE, In-App, Browser Based, Card-on-file, QR, Connected Devices etc.)
- Provide Token Service APIs, interfaces and customer support to stakeholders
- Obtain necessary certifications for the industry compliance
- Maintain Token BINs, PAR support on-behalf of issuers
- Support various cryptographic algorithms for Token transaction processing

Smart Card Alliance

Smart Card Alliance

Security Considerations for Tokenization

John Sheets, Visa

Tokenization vs Encryption – A Common Misunderstanding

- From a security perspective, Tokenization enhances security in an importantly different way than Encryption
- Encryption obfuscates data using an encryption algorithm in conjunction with keys to protect the data
  - While encryption is excellent to ensure confidentiality of the data encrypted, it only protects that data *while it is encrypted*
  - To be used for transaction processing, it is usually the case that the encrypted data must be decrypted to be used, and then re-encrypted to once again protect the data
  - Decrypted data is vulnerable to attack
- In contrast, tokenization **replaces** sensitive data with alternative data that is designed such that it cannot be misused
  - Only the linkage between the token and its original data is sensitive
  - That linkage is stored in the Token Vault

Smart Card Alliance

Tokenization Security Benefits

Token security is based on two key concepts

Identification and Verification (ID&V)

- Provides trusted binding of a payment token to a PAN, supporting a wide range of token business uses

Token Domain Controls

- Restricts use of token to the specific domain for which is was intended
- Domains can be channel-based, merchant specific, require dynamic data included with the token, etc.
- Not all potential restrictions may be required of each token type
- E.g., one token domain may be a specific card-on-file merchant, while another token domain may be for chip card transactions with an accompanying cryptogram

Smart Card Alliance

Tokenization – Additional Security Benefits

Tokenization provides additional security benefits:

Limiting proliferation of PANs

- As the number of devices and places you frequently shop increase, storing PANs in all these places increases risk exposure of the account
- Tokenization addresses this by issuing specific tokens for specific devices and for specific purposes, thereby eliminating PAN data from a merchant environment

Real time token management

- The ability to delete/suspend a token from a device allows for further protection of cardholder accounts when devices are lost or stolen.
- Since different tokens can be assigned to different devices, when one particular device is compromised, only that device needs to be deactivated and other devices do not get impacted.

Tokenization Security - Summary

	Security Measures					
	In-Store			On-Line		
	EMV	Encryption	Tokenization	EMV	Encryption	Tokenization
Counterfeit Cards	✓					
Breach (Data at Rest)		✓	✓		✓	✓
Breach (Data in Flight)		✓	✓		✓	✓
Breach (Data During Use)			✓			✓

Tokenization Security Standards and Guidelines

For those looking for more information on token related security requirements, The PCI council has published PCI TSP Security Requirements. This is available at the PCI council website and is intended for Token Service Providers
https://www.pcisecuritystandards.org/documents/PCI_TSP_Requirements_v1.pdf

Of course the EMV Tokenization framework is available from the EMVCo website for additional information.

Summary & Conclusions

Randy Vanderhoof, Smart Card Alliance

Conclusions and Resources

- Tokenization is a powerful tool which can drastically reduce the risk of payment transaction fraud, especially in mobile and emerging digital payment domains.
- Tokens remove PAN data from the payments eco-system.
- EMVCo has provided a framework for payment tokens which all issuers, processors and acquirers should understand.
- Token security has two main concepts: Identification and Verification (ID&V) and Domain Controls which are essential to proper implementation.
- Token Service Providers play a key role in creating, distributing and providing real-time token management.
- All eco-system participants are encouraged to understand EMV token methods, and implement according to the published standards.

Resources

- **EMVCO Tokenization Framework:** https://www.emvco.com/specifications.aspx?id=263
- Other mobile payments and NFC resources available at: http://www.smartcardalliance.org/publications-payments-mobile-payments-nfc/

Smart Card Alliance

Tokenization Acronyms

Term	Definition
TSP (Token Service Provider)	An entity that provides a Token Service comprised of the Token Vault and related processing. The Token Service Provider will have the ability to create, map, de-map and validate the Tokens to respective payment account numbers.
Token Cryptogram	A cryptogram is a unique value generated using the Payment Token, Keys and additional transaction data to create a transaction specific value.
HCE (Host Card Emulation)	HCE enables contactless payments by emulating contactless service stores the data in the application itself, or they could be stored in other secure locations such as a trusted execution environment (TEE)
TSM (Trusted Service Manager)	An entity that securely provisions the payment credentials inside the Secure Element chips located in the mobile devices.
Identification and Verification (ID&V)	A valid method through which an entity may successfully validate the Cardholder and the Cardholder's account in order to establish a confidence level for Payment Token to PAN / Cardholder binding.
Token Vault	A repository, implemented by a Tokenization system that maintains the established Payment Token to PAN mapping. This repository is referred to as the Token Vault.
Token Requestor	An entity such as mobile wallets that is seeking to utilize Tokenization and initiate requests that PANs be Tokenized by submitting requests to the Token Service Provider.
PAR (Payment Account Reference)	Unique identifier associated with a specific cardholder PAN. This can be used as a reference to all cardholder transactions to leverage for other value added services such as loyalty.
Token Assurance Level	A value that allows the Token Service Provider to indicate the confidence level of the Payment Token to PAN / Cardholder binding based on factors such as Token location etc..

Webinar Project Contributors

- Sadiq Mohammed, MasterCard
- John Sheets, Visa
- Sree Swaminathan, First Data
- Tony Sabetti, CPI Card Group
- Sanjay Varghese, Capgemini
- Lokesh Rachuri, Capgemini
- Suresh Bachu, Discover
- Mike Strock, Smart Card Alliance

Smart Card Alliance

Smart Card Alliance

Q&A

Smart Card Alliance

Randy Vanderhoof
rvanderhoof@smartcardalliance.org

Sadiq Mohammed
sadiq.mohammed@mastercard.com

John Sheets
jsheets@visa.com

Sree Swaminathan
sridher.swaminathan@firstdata.com

191 Clarksville Road
Princeton Junction, New Jersey 08550
WWW.SMARTCARDALLIANCE.ORG