Adam M. Sommer
Business Leader, Industry Standards

MasterCard

Emerging Payments Security

Agenda

- Overview
- EMV
- Tokenization
- P2PE
- Call to Action

Overview

EMV + P2PE + Tokenization

EMV + Tokenization + P2PE

MasterCard

EMV (Chip)

- **Benefit:** Generates a dynamic card authentication value which, if stolen, cannot be used to create counterfeit cards
- **Risk:** Sensitive PAN data is sent in the clear and, if stolen, may be usable for card-not- present fraud (i.e. cross-channel fraud)

Tokenization

- **Benefit:** All token types can remove PAN from the ecosystem.
  - EMV Payment Tokens are unique in providing dynamic cryptograms and domain controls that restrict the use of the data for fraud
- **Risk:** Data exposure risks remain until broad adoption of tokenization is achieved

Encryption

- **Benefit:** Protects sensitive PAN data "in transit" by rendering it unusable if stolen, across all channels. Does not protect data at rest.
- **Risk:** Encryption deployments are not always optimized to achieve full protection and may result in data being in the clear for some portion of transaction processing

A Holistic Approach

	Prevents counterfeit fraud of exposed data?	Protects data in transit?	Protects data at rest?
EMV Chip only	✓	X	X
Encryption + Tokenization	X	✓	✓
EMV Chip + Encryption + Tokenization	✓	✓	✓

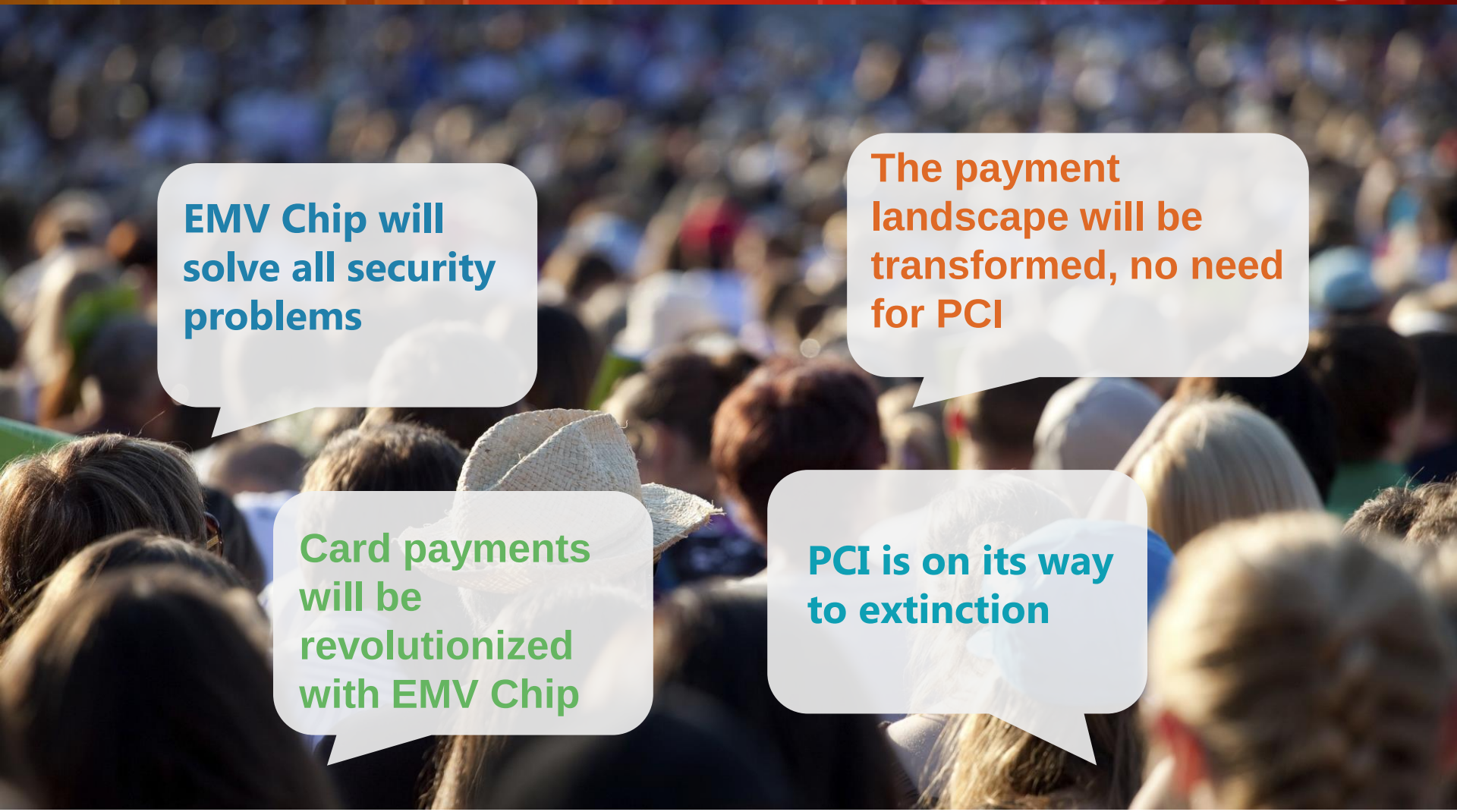
EMV

EMV Needs PCI DSS

MasterCard

EMV Chip Helps Reduce Face-to-Face Fraud

EMV Chip and PCI



MasterCard

EMV Chip Needs PCI

EMV Chip and PCI

What is the impact of EMV?

PCI Standards will continue to evolve…

And will be applied as required, such as with EMV chip

Tokenization

What is Tokenization?

MasterCard

Tokenization replaces valuable information (such as Primary Account Number (PAN) and Expiration Date, or any other sensitive data) with surrogate values that, if compromised, reduce the impact of subsequent fraud

- Surrogate values vary in format and may be cryptographically or non-cryptographically generated – varies by type of token, use case and solution
- Mapping of tokens to PAN and other data occurs within the secure confines of a token vault

Three Token Categories

MasterCard

Payment Tokens – Acquiring Tokens – Issuing Tokens

- Various forms of tokenization have existed for over 10 years and have been used in a number of different payment contexts
- Tokenization is a very broad term which requires understanding the type of token and use case to determine the security impact and value proposition

Different Token Types will and can co-exist

Payment Tokens

MasterCard

EMV Payment Tokens

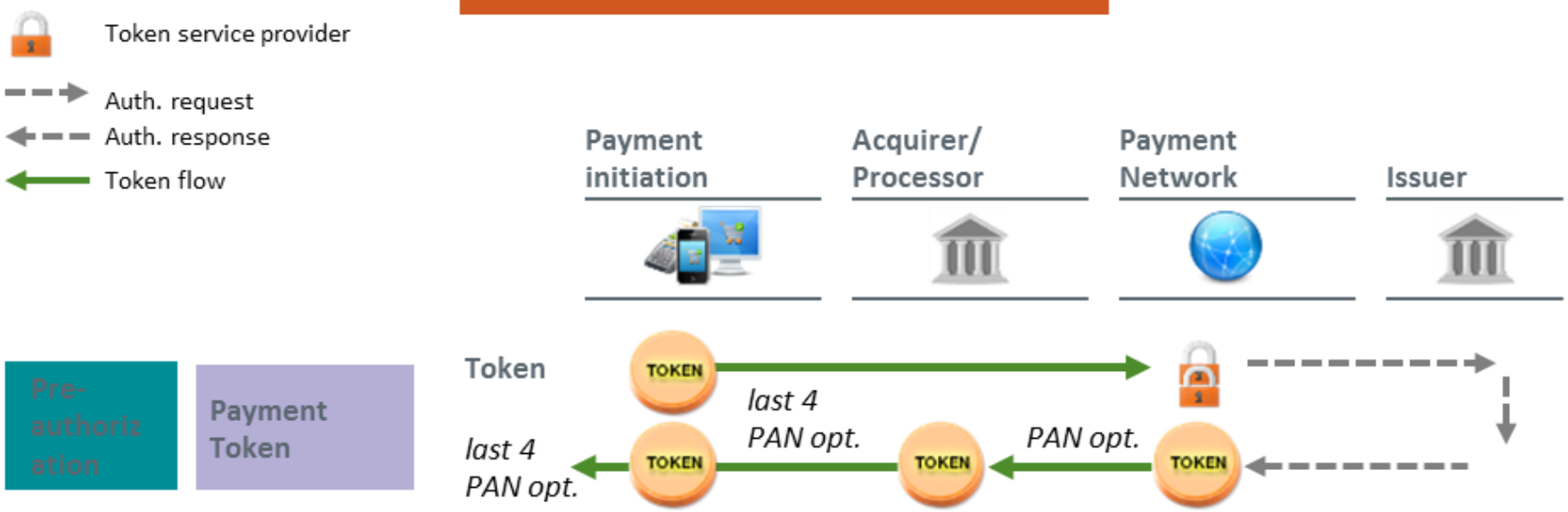
Background

- A token created by or on behalf of an issuer, in accordance with the "EMV Payment Tokenization Specification"
- These tokens offer unique domain controls and dynamic token cryptograms to limit fraud potential

Security Implication + Use Case

- EMV tokens provide protection from the moment of initiation to subsequent de-tokenization in the secure token vault
- Merchant and acquiring environments only have access to the token, thus protecting data at rest and in transit

Token Transaction Flow



Payment Tokens

MasterCard

EMV Payment Tokens

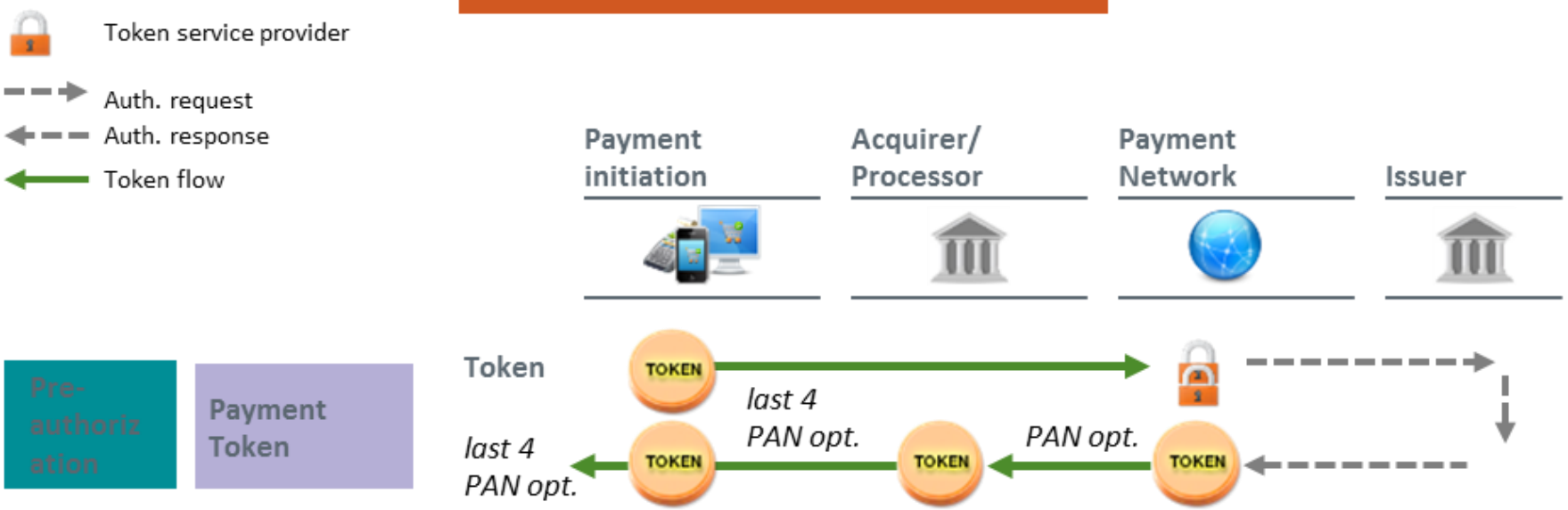
Background

- A token created by or on behalf of an issuer, in accordance with the "EMV Payment Tokenization Specification"
- These tokens offer unique domain controls and dynamic token cryptograms to limit fraud potential

Security Implication + Use Case

- EMV tokens provide protection from the moment of initiation to subsequent de-tokenization in the secure token vault
- Merchant and acquiring environments only have access to the token, thus protecting data at rest and in transit

Token Transaction Flow



Acquiring Tokens

Acquiring Token

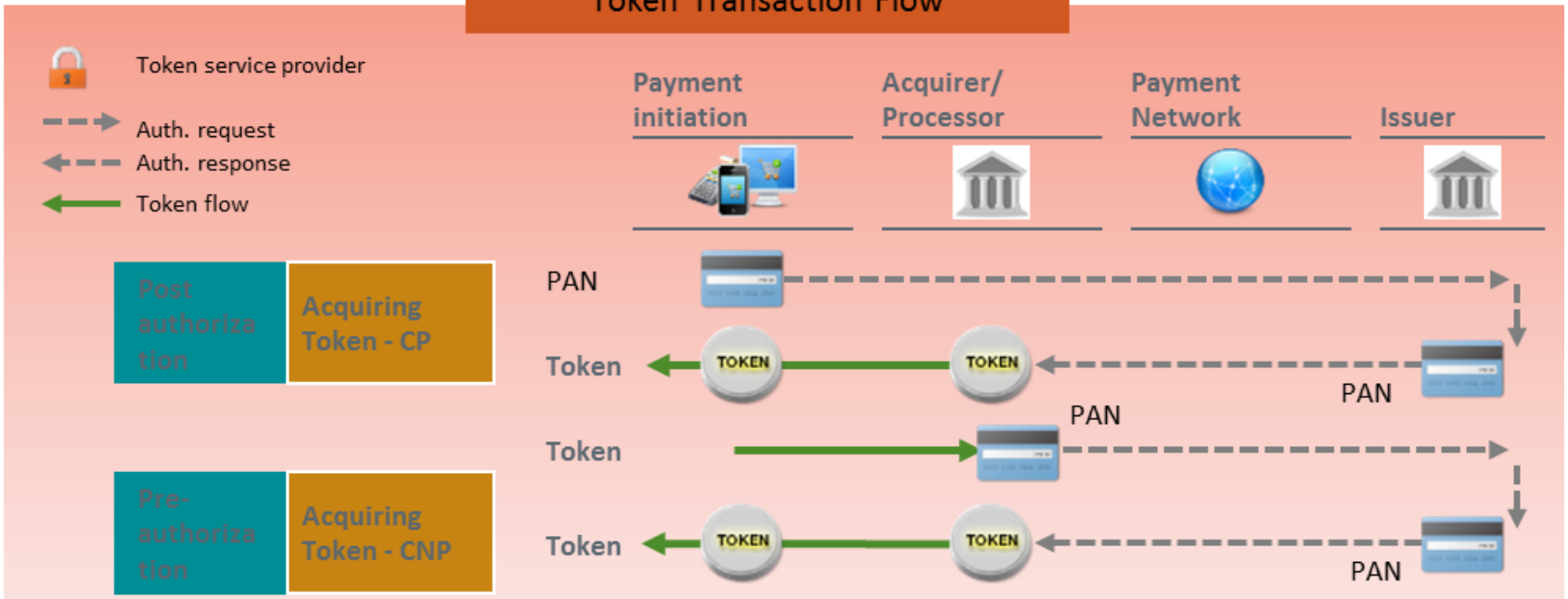
Background

- Acquiring tokens replace sensitive data after card presentment within the closed environment between the acquirer and merchant, within a merchant environment, or within a service provider environment

Security Implication + Use Case

- Acquiring tokens allow the entity to remove sensitive data from storage and may also protect data in transit in certain use cases

Token Transaction Flow



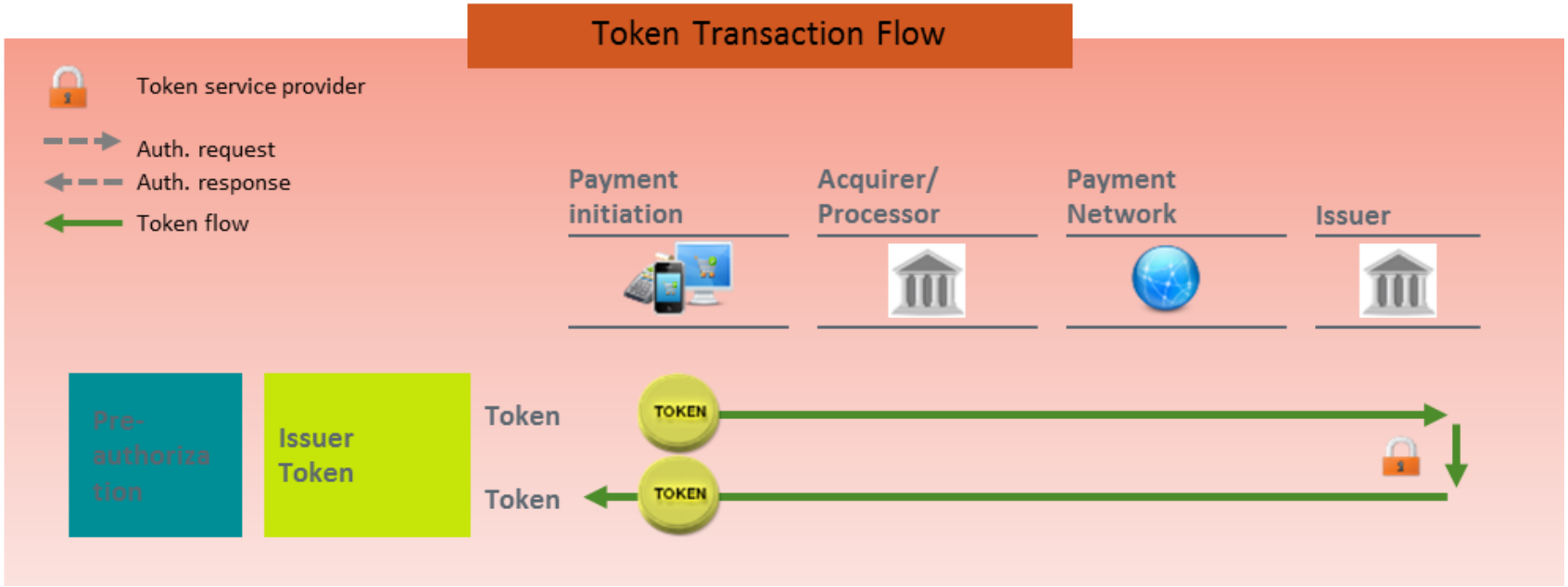
Issuing Tokens

Background

- Tokens that are created by an issuer yet resemble a Primary Account Number (PAN). Also known as Virtual Card Numbers

Security Implication + Use Case

- Issuer tokens provide issuers with means of reducing risk in specific use cases



P2PE

The Point-to-Point Landscape

Point to Point Encryption (P2PE) protects data in transit

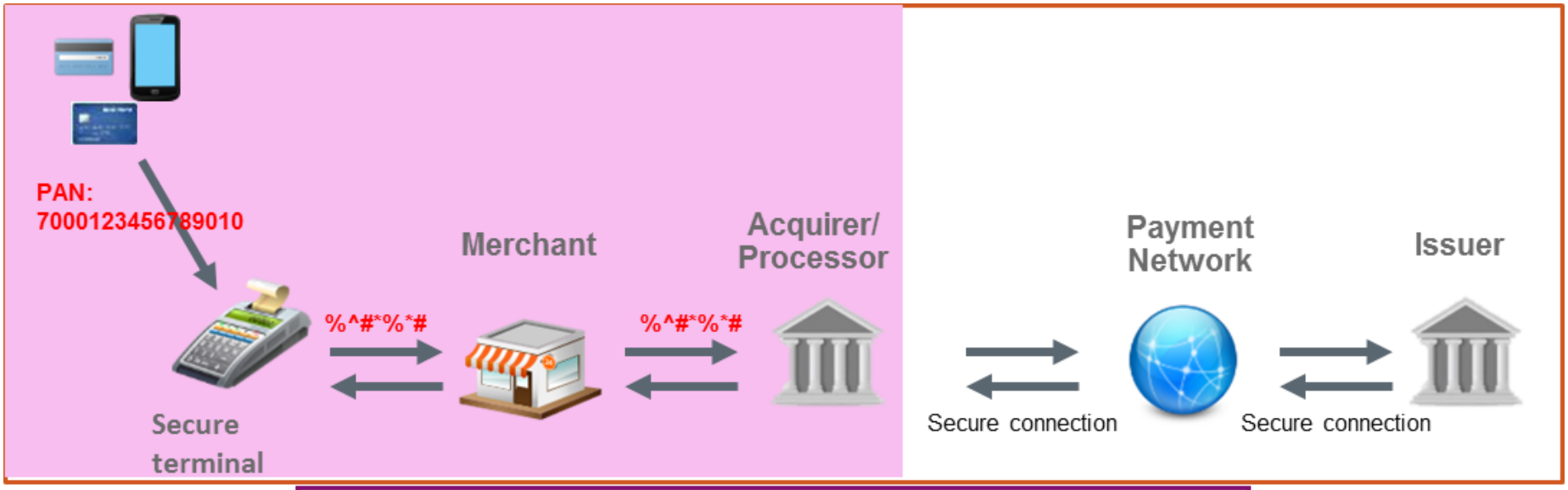
Often bundled with Acquiring Tokens and Accommodates Payment Tokens

Existed in market for 5+ years

Generally offered by Acquirers and Processors

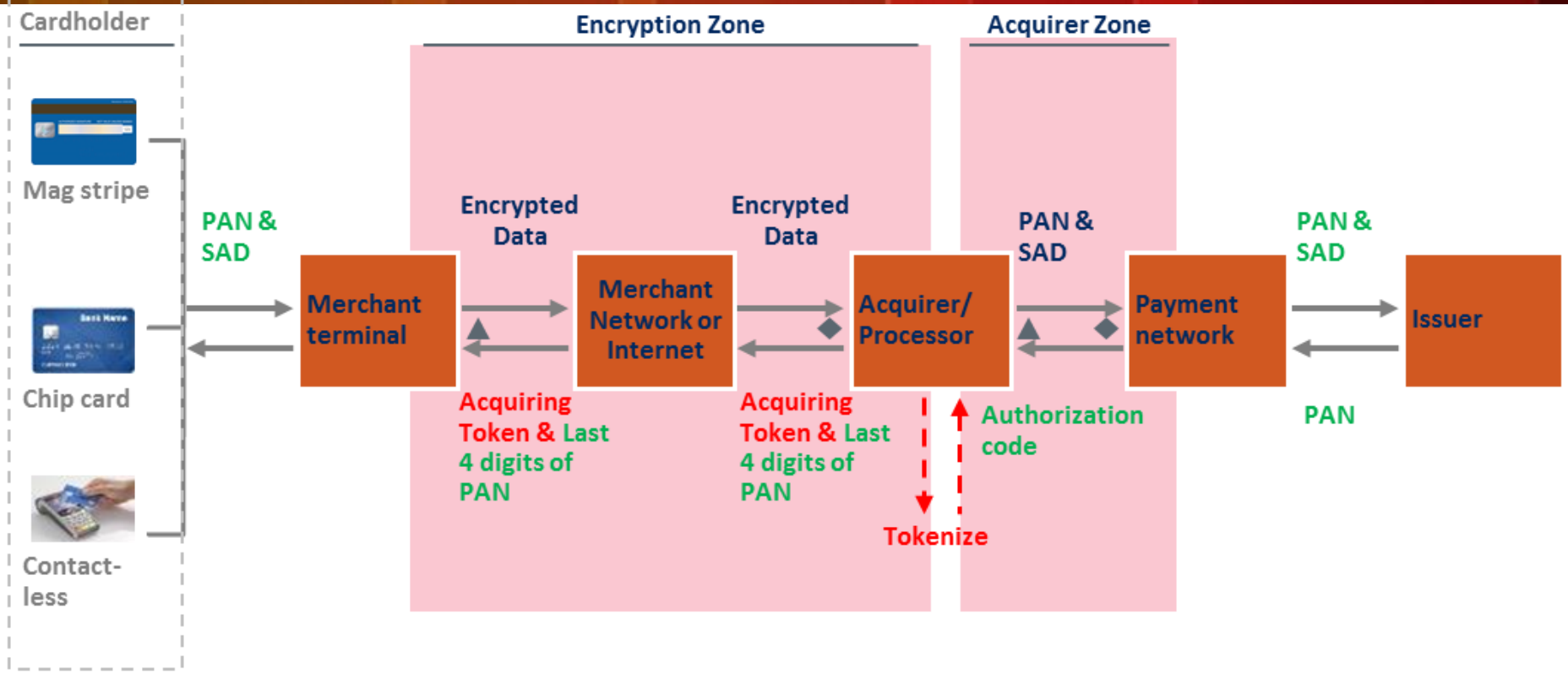
P2PE as a Standalone Solution

- Encryption protects cardholder data starting at the terminal and while “in transit” to the acquirer.
- Encrypts PAN, Sensitive Authentication Data (SAD), expiration date, full track data, track equivalent data as well Personally Identifiable information (PII) and all token types



- Encryption is best deployed within a secure terminal as opposed to elsewhere within the POS system

P2PE + Tokenization



- Data is encrypted in terminal
- Encrypted data is protected in transit
- Data is decrypted in a secured decryption zone

Auth. request
Auth. response
Cryptographic Zones

XXX Card data
XXX Encrypted data
Encryption point
Decryption point

Standards

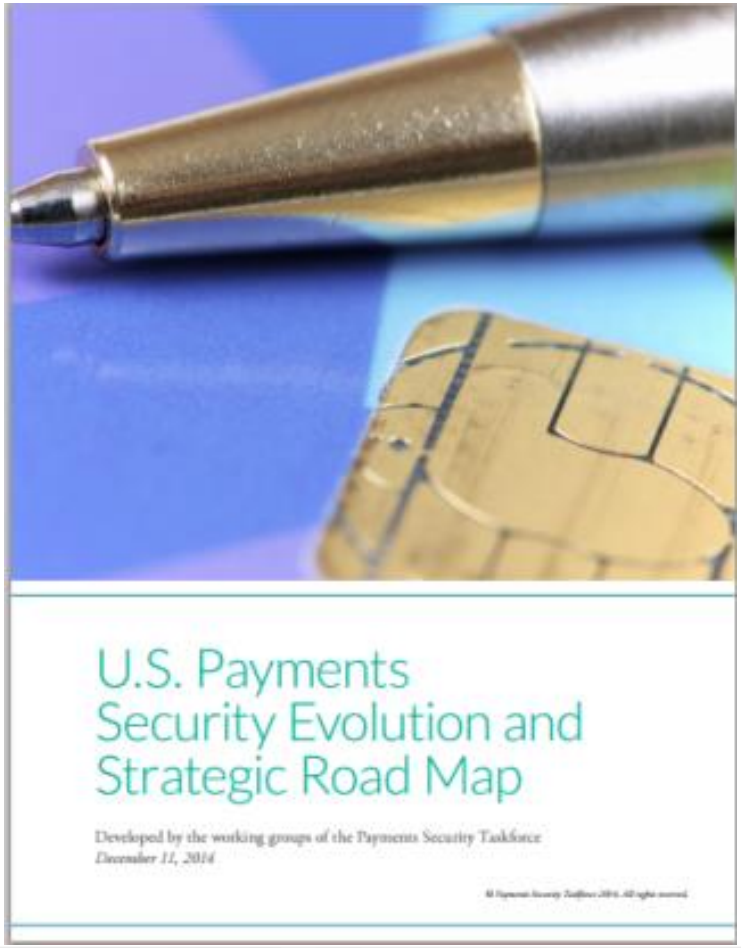
MasterCard

PCI Security Standards Council Update

- Developed Standards and Listing Program for P2PE Solutions in 2012
- Released V2.0 of Standard in 2015 based upon industry collaboration
  - Increased Flexibility
  - Improved Simplicity

Call to Action

US Payment Security Taskforce



http://newsroom.mastercard.com/wp-content/uploads/2014/12/US-Payments-Security-Evolution-and-Strategic-Road-Map-for-Release1.pdf

Additional Resources

The SDP Website

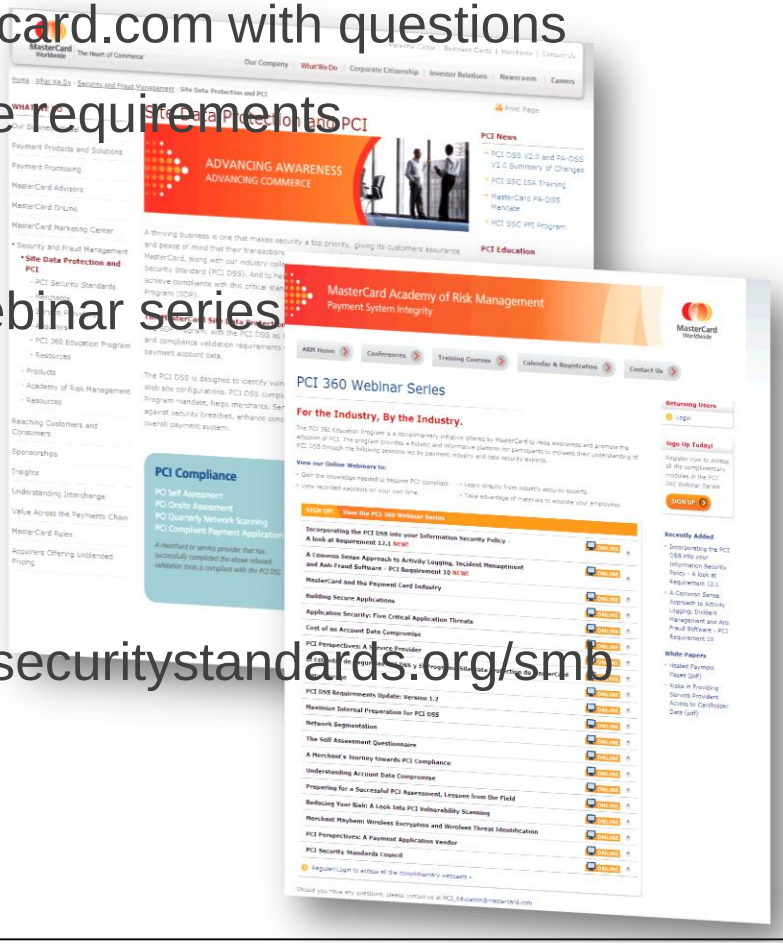
- SDP Program information – sdp@mastercard.com with questions
- Merchant level definitions and compliance requirements

PCI 360

- Complimentary access to our PCI 360 webinar series

PCI Security Standards Council

- **PCI SSC Merchant Resource Website** : www.pcisecuritystandards.org/merchants
- **PCI SSC Small Merchant Site**: www.pcisecuritystandards.org/smb



Thank You!