

PCI Point To Point Encryption (P2PE) An Overview

Moderator Name: **Erik Winkler**

Panelists Names: ***Sonjay Shepherd*** – *HiTouch Business Services*,
Adam Sommer – *MasterCard*



Definition of Account Data



Account Data consists of cardholder data and/or sensitive authentication data

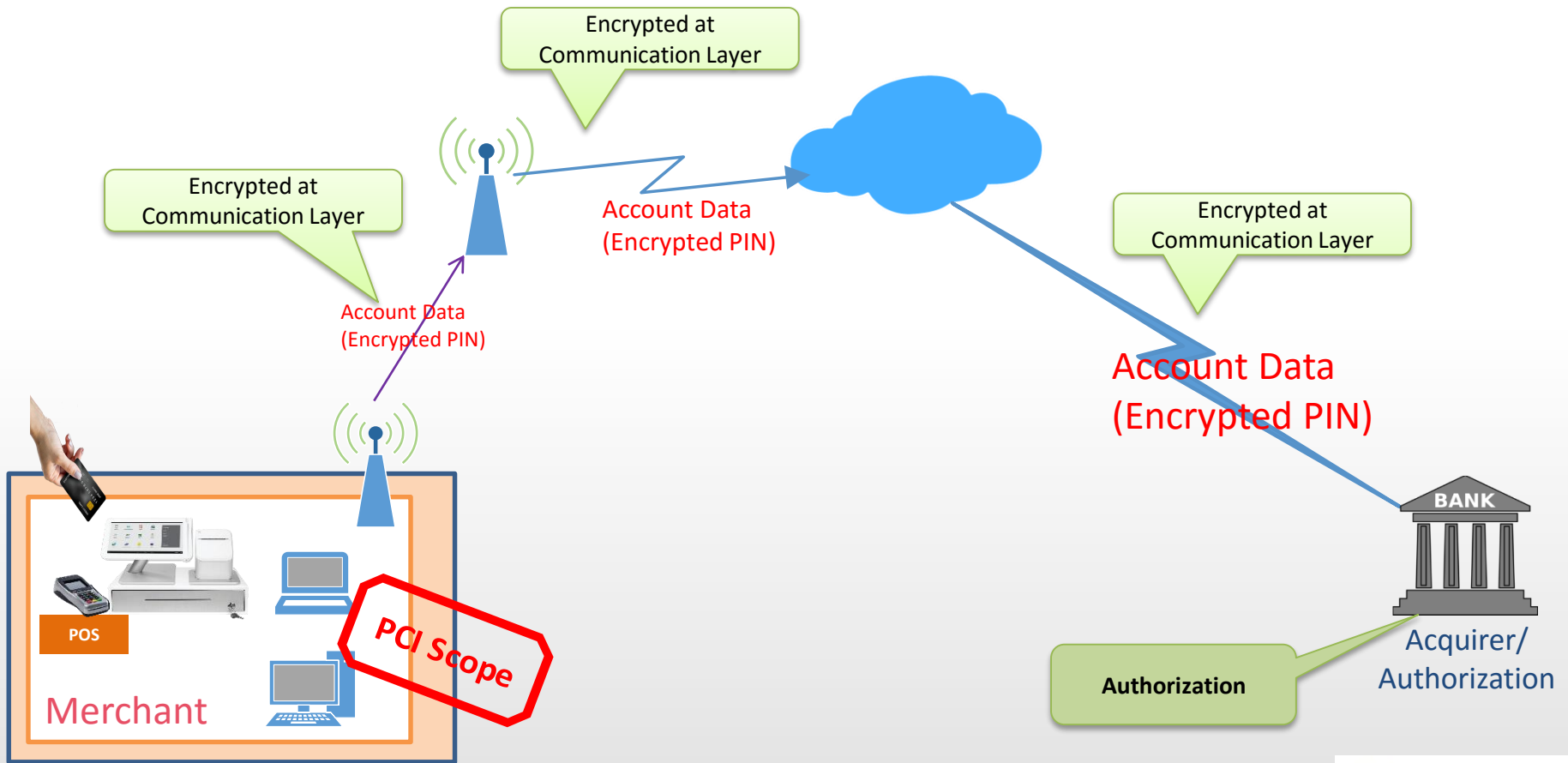
Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
Primary Account Number (PAN)	Full Magnetic Stripe Data
Cardholder Name	or Equivalent on a Chip
Expiration Date	CAV2/CVC2/CVV2/CID
Service Code	PINs/PIN block



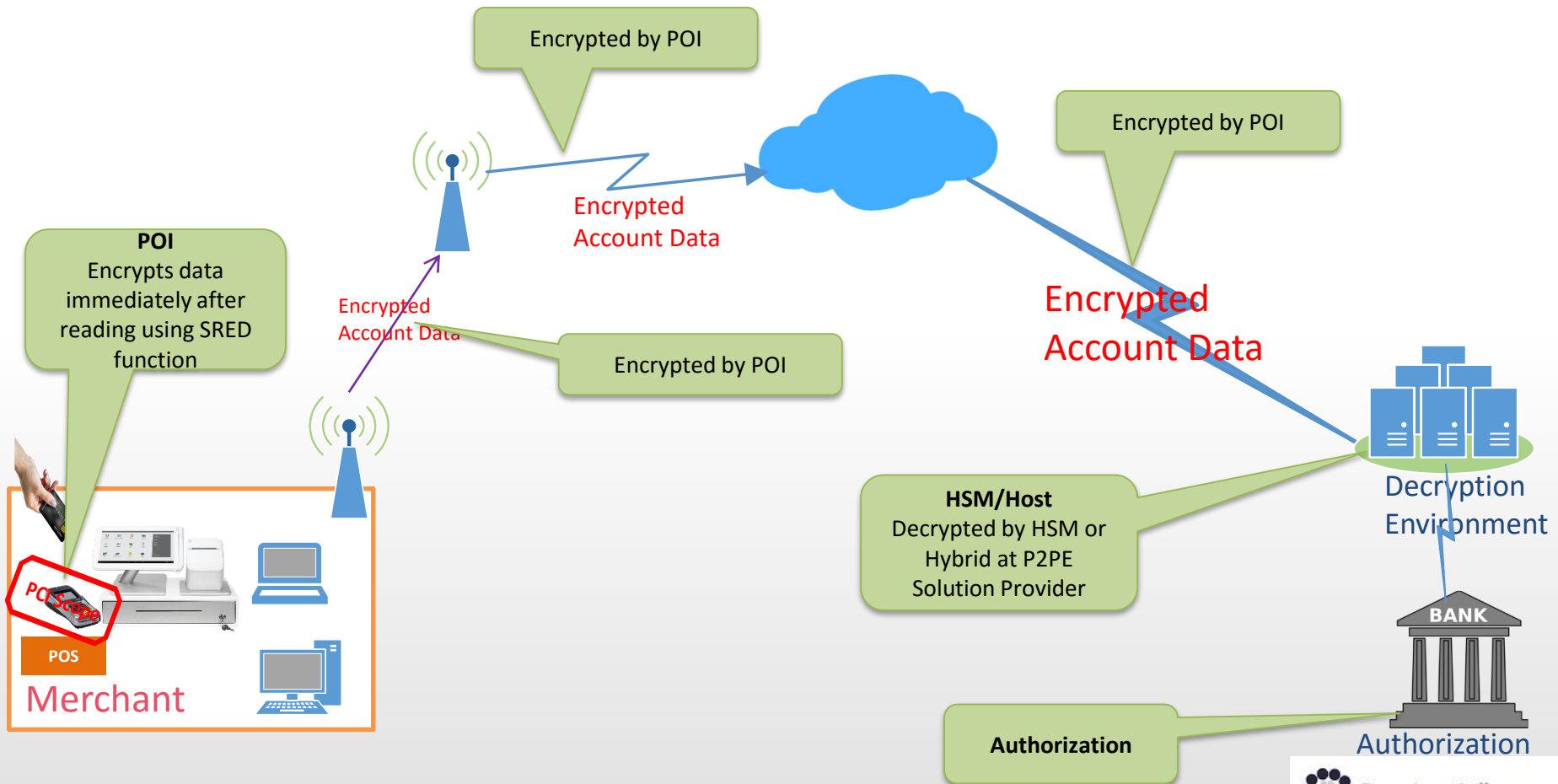
What is P2PE?

- A point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption.

Typical Payment Method



Payment Method in P2PE



Who should consider P2PE?

This is intended for Merchants

- ✓ Better Security
- ✓ Easier Compliance
- ✓ More options

P2PE Solution overview

Typical data-flow:


Merchant Environment



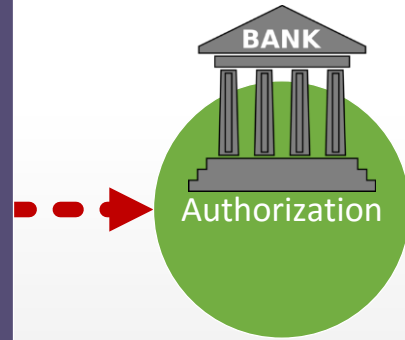
PTS approved POS with SRED



P2PE Solution Provider

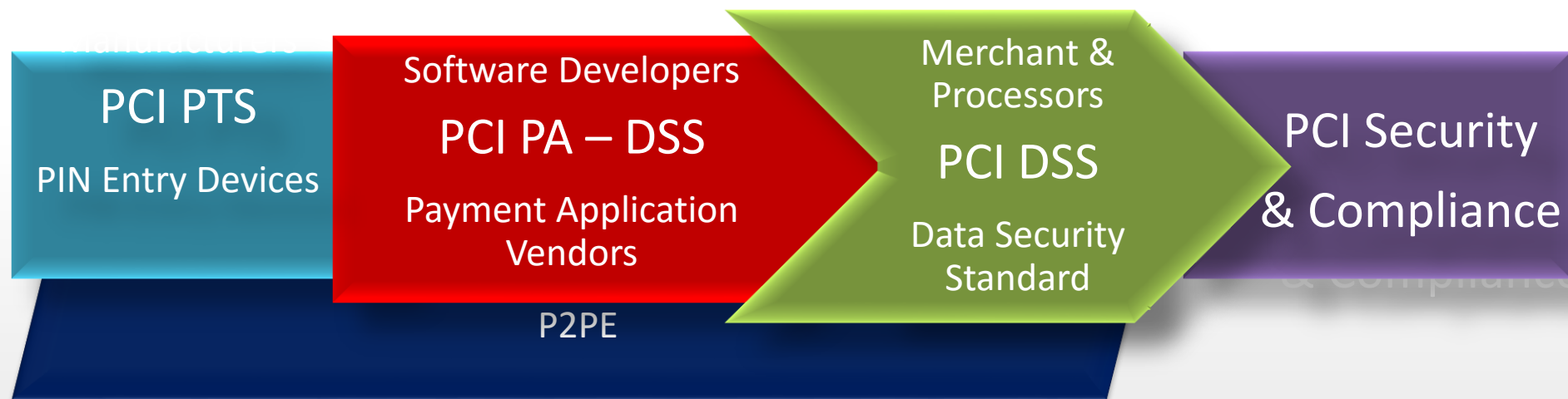


Decryption Environment



PCI Family of Standards

Ecosystem of payment devices, applications, infrastructure and users



Benefits of P2PE

- ❖ Offers a powerful, flexible solution for all stakeholders
- ❖ Makes account data unreadable by unauthorized parties
- ❖ Reduces fraud and theft
- ❖ Protects customer data and client reputation
- ❖ Simplifies compliance with PCI DSS
- ❖ Recognized by all Participating Payment Brands

Description of P2PE

- **It is either a solution or Application.**

- **P2PE Solution**

A point-to-point encryption solution consists of point-to-point encryption and decryption environments, the configuration and design thereof, and the P2PE Components that are incorporated into, a part of, or interact with such environment.

- **P2PE Application**

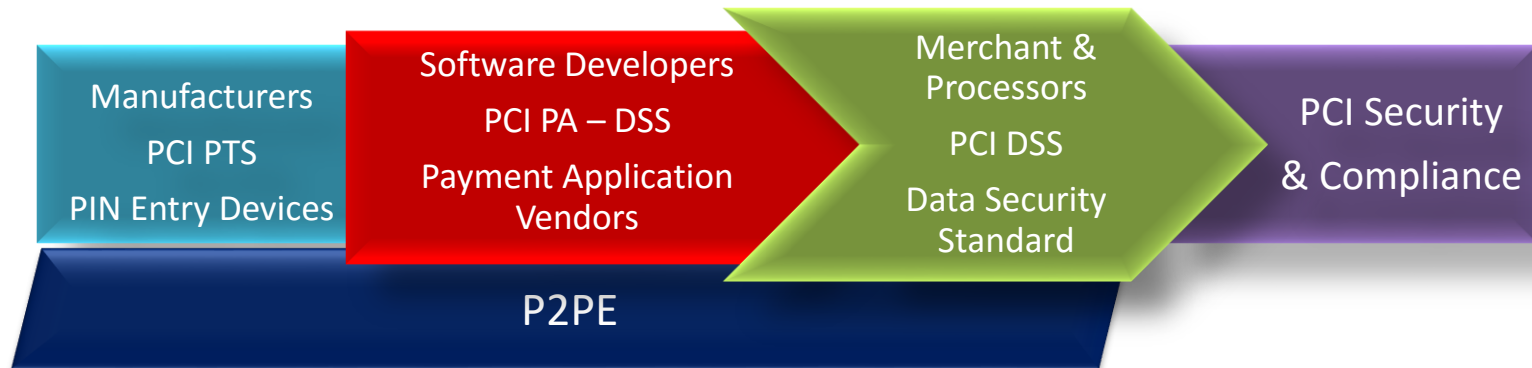
A software application that is included in a P2PE Solution and assessed per P2PE Domain 2 Requirements, and is intended for use on a PCI-approved point-of-interaction (POI) device or otherwise by a merchant.

- **P2PE Components**

Any application or device that stores, processes, or transmits account data as part of payment authorization or settlement, or that performs cryptographic key management functions, and is incorporated into or a part of any P2PE Solution.

Component of P2PE

Ecosystem of payment devices, applications, infrastructure and users



- POI approved by PCI PIN Transaction Security (PTS) POI
- HSM for decryption approved by PCI PTS HSM
- Key Operation derived from PCI PTS PIN standard
- POI Application aligns with PA DSS
- Decryption environment conforms with PCI DSS

ControlCase P2PE offerings

- Guidance on designing P2PE Solutions
- Review of P2PE Solution design
- Guidance on preparing the P2PE Instruction Manual
- Pre-assessment (“gap” analysis) services
- Guidance for bringing the P2PE Solution into compliance with the P2PE Standard if gaps or areas of non-compliance are noted during the assessment.
- Certifying P2PE solutions and Applications

Q & A

