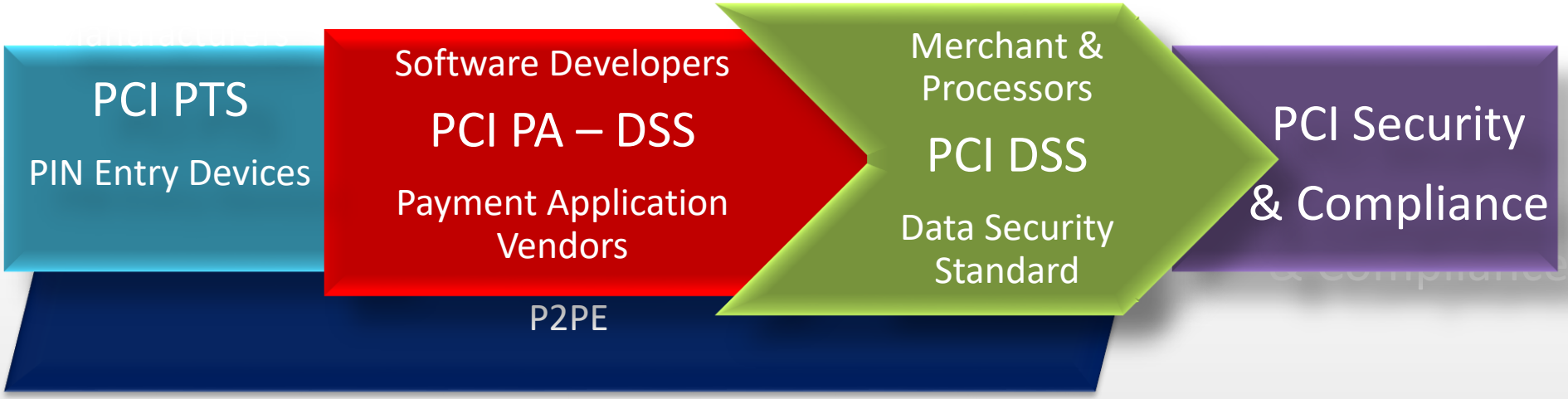
ControlCase
Compliance as a Service

Advanced Certifications – PA-DSS and P2PE

Erik Winkler, VP, ControlCase

PCI Family of Standards

Ecosystem of payment devices, applications, infrastructure and users



ControlCase
Compliance as a Service

PA-DSS and P2PE Protect Account Data

Account Data consists of cardholder data and/or sensitive authentication data, all information printed on the physical card and data on the magnetic strip and chip.

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

ControlCase
Compliance as a Service

PA-DSS Certification

Payment Application Compliance

ControlCase
Compliance as a Service

What is PA-DSS?

- The Payment Application Data Security Standard (PA-DSS) applies to all payment applications that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) as part of authorization or settlement.
- These applications are typically sold and installed "off the shelf" without pre-installation customization by vendors.

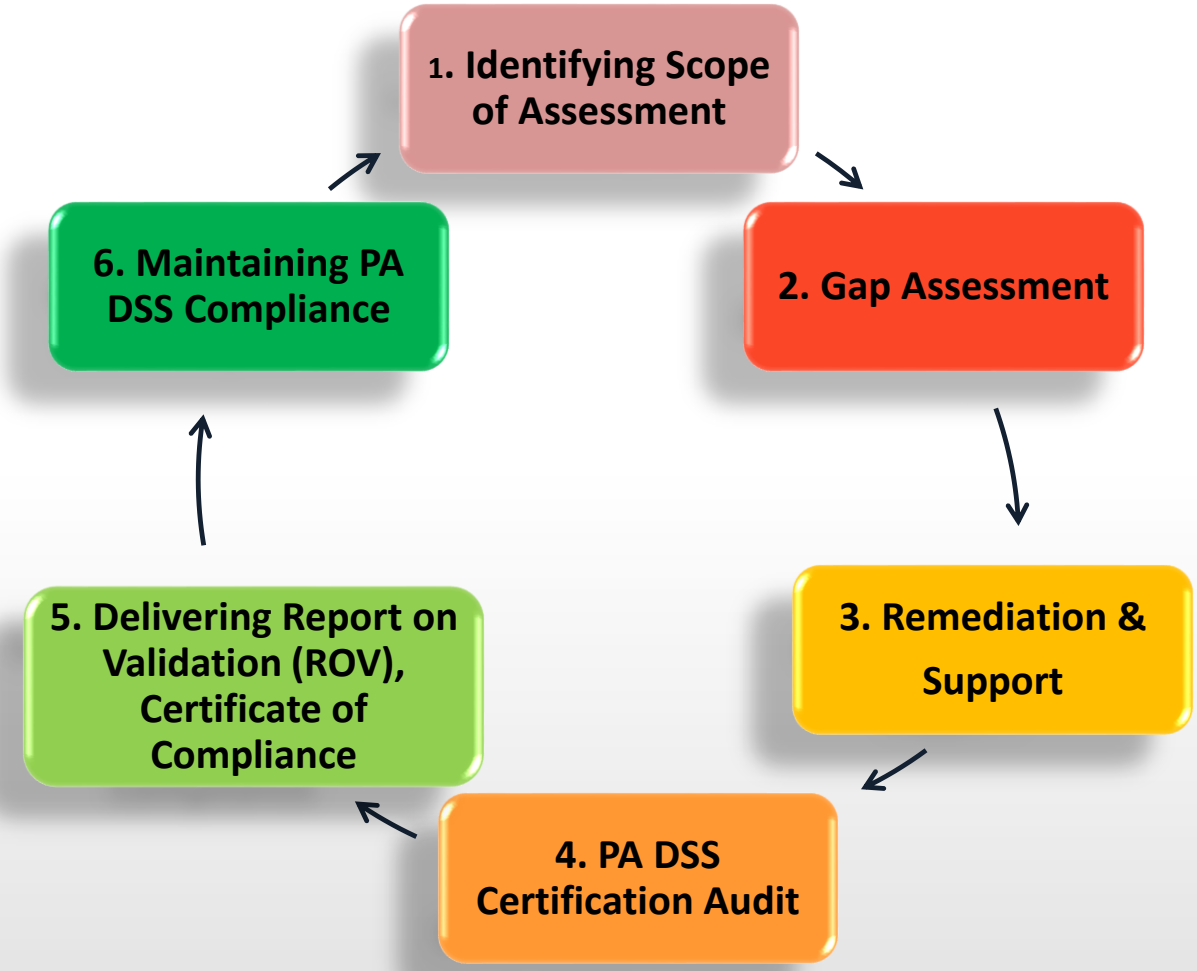
ControlCase
Compliance as a Service

When is PA-DSS Not Applicable?

- PA-DSS does NOT apply to applications in the following instances:
  - Applications offered as a service.
  - Applications built for a single end-user customer.
  - Applications developed for in-house use only.
  - OS where the payment application is installed.
  - Databases or back-office systems that store cardholder data.

ControlCase
Compliance as a Service

PA-DSS Assessment



ControlCase
Compliance as a Service

Benefits of PA-DSS

- Ensures that the payment application can be implemented and operated in a PCI DSS compliant manner.
- PA-DSS certified applications are recognized by the participating card brands as meeting security mandates regarding storing of SAD.

ControlCase
Compliance as a Service

ControlCase PA-DSS Offerings

- PA DSS Gap Analysis
  - Identification of non-compliant areas
  - Recommended approach for remediation
- PA DSS Remediation Support
  - Implementation Guide
  - Addressing non-compliant areas of the application
- PA DSS Final Audit and Report on Validation (ROV) / Attestation of Validation (AOV) preparation and submission to PCI SSC

ControlCase
Compliance as a Service

P2PE Certification

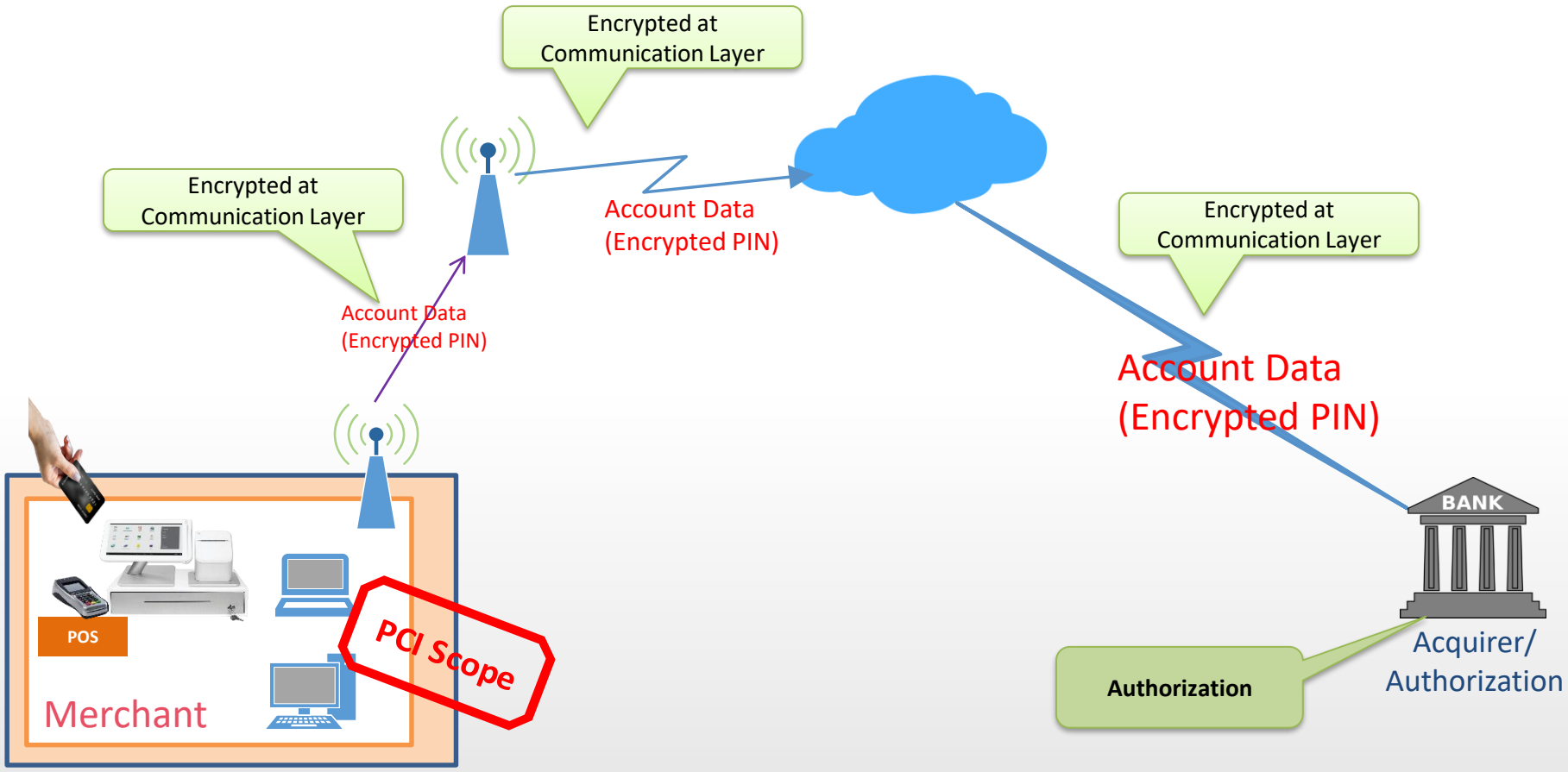
Understanding the Basics

ControlCase
Compliance as a Service

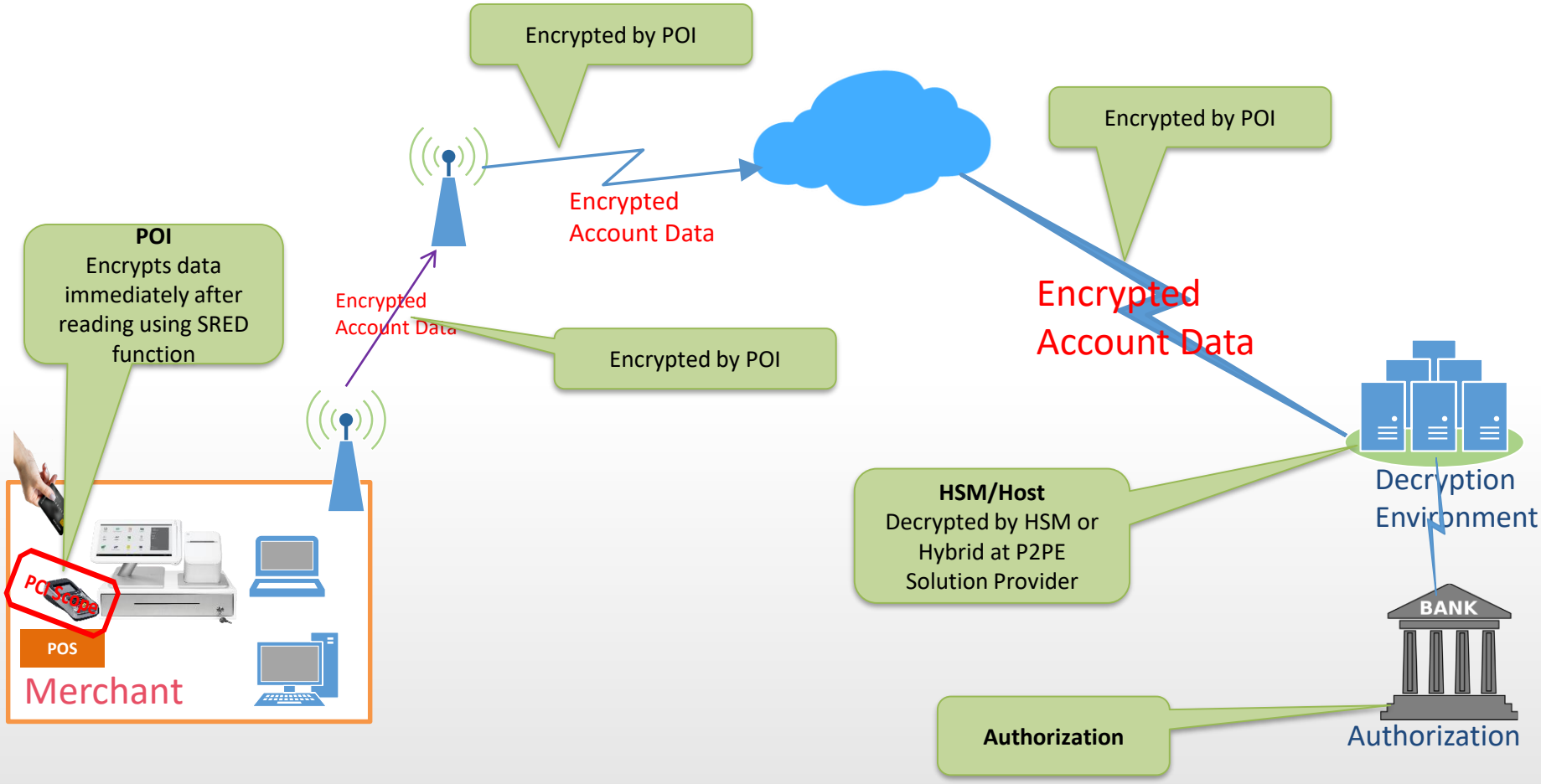
What is P2PE?

- 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



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

ControlCase
Compliance as a Service

P2PE Domain Summary

6 Domains

Domain 1

Encryption Device and Application Management

Domain 2

Secure Application Development

Domain 3

P2PE Solution Management

Domain 4

Merchant-managed Solutions

Domain 5

Decryption Environment

Domain 6

P2PE Cryptographic Key Operations and Device Management

ControlCase
Compliance as a Service

P2PE – Key Summary Points

- Allows merchants to use the SAQ P2PE if they qualify.
- Current version 2.0 Revision 1.1 – Released in July 2015
- P2PE scenarios (e.g. Hardware Decryption or Hybrid Decryption)
- Requires the use of HSM for management of cryptographic keys.
- POI devices must be PCI SSC approved PTS devices with SRED (secure reading and exchange of data) listed as a "function provided."
- HSMs must be either FIPS 140-2 Level 3 (or higher) certified or PCI-approved
- Applications with access to clear-text account data must undergo validation per all P2PE Domain 2 Requirements

ControlCase
Compliance as a Service

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

ControlCase
Compliance as a Service

Q & A