# EMV, PCI, Tokenization, Encryption
## *What You Should Know for 2015*

Presented by:

The Bryan Cave Payments Team

BRYAN CAVE

*A Broader Perspective*℠

# Agenda

- Overview of Secured Payments – Judie Rinearson (NY)
- EMV – Courtney Stout (DC)
- End to End Encryption – Jennifer Crowder (KC)
- Tokenization – Jennifer Crowder (KC)
- Implementation – Courtney Stout (DC)
- Third Party Contract – John ReVeal (DC)
- Conclusion – John ReVeal (DC)

Judith Rinearson, New York

# SECURED PAYMENTS OVERVIEW

# Securing Merchant Payments – Benefits and Challenges

- Substantial emphasis in payments industry on securing payments.
- Two goals – preventing fraud and data breaches.
- Will address benefits and challenges of each, issues for merchants upgrading their systems, and the legal and contractual issues that must be addressed along the way.

# Fraud Prevention

- Fraud prevention involves implementing efforts to authenticate to validity of the payment card and the customer's right to use the card.
- Current focus – EMV. EMV validates a card (through the check of the chip data) that a card is not invalid or stolen, and validates the user through the PIN.
- In Europe, once EMV implemented, fraudsters turned their focus to online fraud prevention.

# Data Breach Prevention

Several focuses:

- End-to-End (or point to point) Encryption
- Tokenization
- Not receiving or storing sensitive data at all

# Outline

Today's Presentation will cover:

- What is EMV?  What are the benefits of EMV?
- What is End-to-End (E2E) Encryption?
- What are the benefits and challenges of E2E Encryption?
- What is tokenization?  How does it fit in?
- How does a merchant bring it all together?
- What do you need to consider if you're contracting with a third party?

Courtney Stout, Washington, DC

# WHAT IS EMV?

# What is EMV?

- **EMV is a chip technology that is becoming the global standard for credit and debit card payments.**
  - The payment instruments contain embedded microprocessor chips.
    - Chips store cardholder data.
    - Chips provide dynamic (e.g., changing) authentication.
  - Benefits include increased security, reduced fraud and new payment methods.
  - The U.S. is late to the game in adopting EMV.
  - "EMV" is named after the original developers of the smart chip technology - Europay, MasterCard and Visa.
  - "EMV" is also referred to as: smart card, smart-chip card, EMV smart card, EMV card, "chip and PIN", "chip and signature", or chip enabled card.

# How are EMV Cards Different?

- **Why are EMV cards more secure than traditional cards?**
  - Traditional cards contain unchanging payment card data on a “magnetic stripe”.
  - Anyone accessing the “magnetic stripe” data gains the card data necessary to make purchases.
  - Every time an EMV card is used for payment, the chip creates a unique transaction code that cannot be used again.
- **How do EMV transactions work?**
  - Both the EMV card transaction and the magnetic stripe transaction have two basic steps: the card is read and then the transaction verification is completed.
  - Consumers will no longer “swipe” their payment card.
  - Data is transmitted between the card and the issuing bank (or other database) to verify the card and to create the unique transaction data for the purchase.

# Why Move to EMV?

- **Driven by Payment Card Network Milestones**
- **Liability shift occurs effective October 2015: The payment card network rules contain provisions that shift liability for fraudulent card transactions.**
  - Under current rules, consumer losses from counterfeit fraud fall back on the issuing bank or the processor.
  - U.S. deadline of October 1, 2015, for a “fraud liability shift”.
  - Liability for “card present” transactions (e.g., in store POS) will shift to whoever is the least EMV-compliant in the payment chain.
  - So, if a merchant has not implemented EMV card readers, the liability for the card fraud will shift to the merchant after October 1, 2015.

# Card Network Rules – EMV Liability Shift

- **Visa:** The party at fault for a "chip-on-chip transaction" not occurring will be liable.
- **MasterCard:** The party who does not support EMV assumes liability for counterfeit card transactions. MasterCard supports a liability shift for lost, stolen, and never received or issued (NRI) cards to the party that does not support PIN as a cardholder verification method. MasterCard offers additional incentives to merchants to encourage rapid EMV adoption.
- **American Express:** The party that has the most secure form of EMV technology will have the least responsibility for certain types of fraudulent transactions.
- **Discover:** The party with the highest level of available payments security benefits from the fraud liability shift.

# President Obama's Executive Order – October 17, 2014

- Intended to improve the security of consumer financial transactions.
- Requires all federal agencies to begin, as soon as possible, a transition to chip-and-PIN technology.
- Effective immediately, new Direct Express® prepaid cards must have enhanced Chip & Pin security features. By 1/1/2015 must have a plan to replace all existing non-chip and PIN Direct Express Cards.
- Increased efforts to assist victims of identity theft.
- Also, plans to ensure that federal agencies with access to personal data require the use of multiple factors of authentication and an effective identity proofing process.
- http://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security

Jennifer Crowder, Kansas City

# ENCRYPTION AND TOKENIZATION

# What is End-to-End Encryption?

- “End-to-End” (E2E) or “Point-to-Point” (P2P) encryption means all data in a particular data flow is encrypted. For example, payment card data either arrives at a merchant encrypted or is immediately encrypted by a merchant upon receipt; then this encryption is maintained until the merchant transmits the data to the processor.
- It essentially provides a secure digital “tunnel” through which data can flow securely.

# Goals and Benefits of E2E Encryption

- Data that is accessed by unauthorized third parties cannot be read or used.
- Many of the data breaches of the past few years would have been non-incidents if the data had been encrypted.
- Considered very high security for sensitive data.

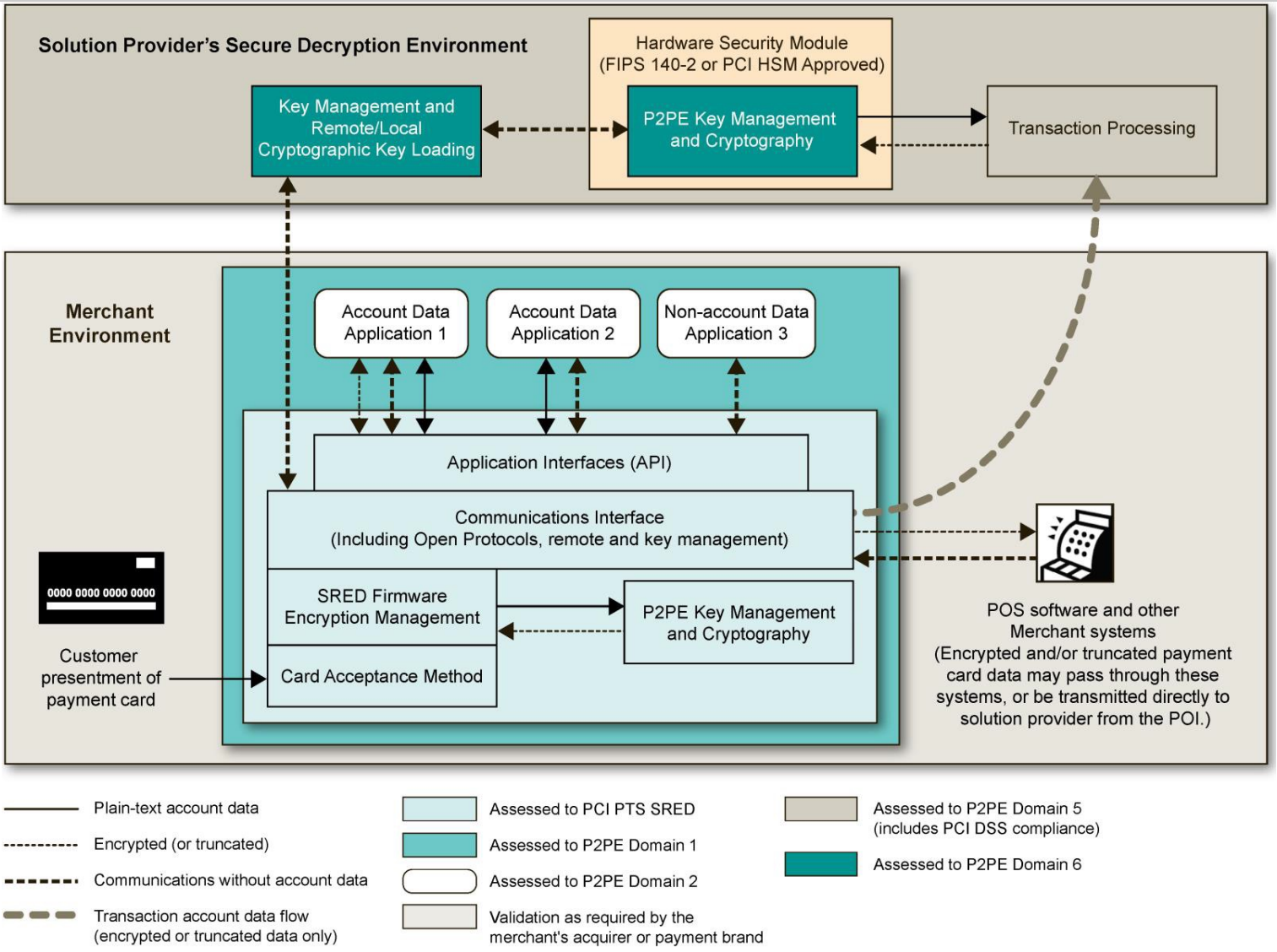
# What do PCI standards say about E2E Encryption?

- PCI Standards recognize that End-to-End Encryption (or Point-to-Point Encryption), is a safer solution.
- Merchants who implement validated encryption programs benefit by receiving a reduced scope for their PCI-DSS assessment. For a reduced scope, requirements *include*:
  - Merchant must use a validated encryption solution.
  - Merchant must never store, process, or transmit clear-text account data within their encryption environment (unless PCI approved).
  - PCI DSS compliance of the decryption environment must be confirmed on an annual basis.
- Source: https://www.pcisecuritystandards.org/documents/P2PE_v1-1.pdf

# What is required to achieve E2E Encryption goal?

- In the retail environment, entire data flow must be encrypted.
- Card readers must support E2E Encryption technology.
- Readers must be integrated with the host computer and data must move under a bank-approved communications protocol to send and receive authorization requests via a secure global payment gateway.
- While more expensive and time consuming than tokenization, E2E Encryption protects a greater range of data.

# From PCI Security Standards Council:
## Illustration of a "Typical" Implementation



# Tokenization

- What is tokenization?
- PCI Standards Council's view.
- Payment Card Networks' view.

# Tokenization vs E2E Encryption

## Tokenization

**Tokenization Pros**:

- Account data is not stored or sent in its "real" form at all (possibly on the first initial transaction but not afterward).
- Easier to establish and maintain than encryption.

**Tokenization Cons:**

- Typically only account data is tokenized. Does not address all data in use by organizations.
- May not work with applications and processing technologies.

## E2E Encryption

**End to end encryption Pros:**

- Data is secured all the way from each endpoint to the processing destination.
- May integrate better with existing technology.

**End to end encryption Cons:**

- May introduce more overhead in processing.
- Key management and other encryption processes may be hard to manage.

**Source:** http://www.bankinfosecurity.com/tokenization-vs-end-to-end-encryption-experts-weigh-in-a-1869/op-1

Courtney Stout, Washington, DC

# IMPLEMENTATION

# Implementation

- With liability shift, many merchants have sufficient financial incentive to move to EMV.
- Most experts agree that tokenization will be a key part of merchants' security measures in the next 3-5 years.
- With increased data breach risks, and since their collected data goes beyond payment card data, merchants have incentive to go further and try for E2E encryption.

# Challenges

- Existing infrastructure.
- Existing payments equipment and services contracts.
- Uncertainty of which providers will provide long term solution.
- Need to keep up with changing payment card network requirements and benefits eligibility. To some extent payment card networks may “pick winners”.
- Hard to conduct cost benefit analysis since rules are still developing.

John ReVeal, Washington, DC

# THIRD PARTY CONTRACTS

# Selecting Providers

- Perform appropriate due diligence in selecting third parties.
  - Evaluate the third party's legal and regulatory compliance program and expertise.
  - Evaluate the third party's depth of resources and previous experience in the specific area, obtain reference checks, review regulatory filings when available.
  - Assess their financial condition, including through reviews of audited financial statements.

# Selecting Providers

- Perform appropriate due diligence in selecting third parties (continued).
  - Ensure the third party periodically conducts thorough background checks on its senior management and employees, as well as subcontractors.
  - Assess the provider's information security systems.

# Selecting Providers

- Perform appropriate due diligence in selecting third parties (continued).
  - Evaluate the provider's business resumption and contingency planning policies, procedures and systems.
  - Verify that the provider has appropriate fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligence, and hazard insurance covering fire, loss of data, and protection of documents.

# Provider Contracts

- Clearly address the nature and scope of the arrangement.
  - Identify the specific services.
  - Be clear on who provides what facilities and equipment.
  - Address compliance with laws.
  - Address the ability to subcontract services.

# Provider Contracts

- Include performance measures or benchmarks.
- Ensure that the contract requires the provider to create and maintain appropriate records.
- Include the right to audit and to require remediation.
  - If third party audits will be relied on, ensure that they appropriately address technology and security standards.
- Address responsibilities and cost allocations for changes required due to new or amended regulations.

# Provider Contracts

- Include business resumption and contingency plan requirements.
- Require the provider to maintain adequate insurance and to provide evidence of coverage where appropriate.
- Consider whether to provide for arbitration.
- Be clear on events of default and the standards for termination of the contract.

# Moving Forward

- The RFI, RFP processes.
- Contracting with providers.
  - Challenge of legacy systems and providers
  - Requirement to maintain compliance with PCI and payment card network rules
  - The gamble of upgrading systems in ever-changing environment
  - What can you expect from providers to address these issues?

# Conclusion

- Increasing Security
- Preventing Fraud
- Complying with network rules

- Save the Date for Future Webinars:
  - *How to be Ready for Legal Issues that Arise in a Data Incident* – Tuesday, January 27th
  - *Key Issues in Money Transmitter Licensing* – Thursday, February 19th