EMV 101 – What You Need to Know Before the October Deadline

September 2, 2015

TRANSFIRST®

First In Secure Electronic Payments

NFIB
The Voice of Small Business®

TRANSFIRST®
First In Secure Electronic Payments

Welcome!

TRANSFIRST®
First In Secure Electronic Payments

Introduction to EMV

1. What is EMV®?
2. Status of the U.S. migration to EMV
3. Touch points on the impact EMV will have on the U.S. payments infrastructure
4. What EMV is not
5. What EMV will solve over time
6. Additional considerations for EMV adoption urgency for merchants
7. EMV implementation models
8. Appendix information and timelines from the card brands

What is EMV?

EMV is:

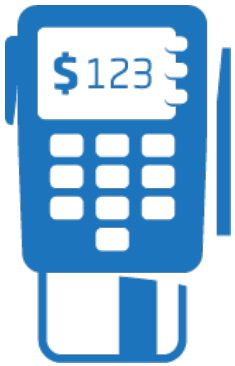
- An acronym created by Europay®, MasterCard® and Visa®
- The global standard for the implementation of chip cards for the purpose of facilitating a more secure electronic payment transaction
- A security framework that defines the payment interaction at the physical, electrical, data and application levels between chip cards and payment devices

EMV is also known as “chip and PIN” in the U.K.; domestically, EMV may be implemented as chip and PIN, chip and signature, or other variations.

Secure Chip Card Technology

EMV-enabled cards — also known as chip cards or smart cards — have an embedded secure microprocessor chip that stores cardholder data and creates a unique value to make each processing transaction unique. This is known as dynamic authentication.

Smart Cards Can Be:



"Contact"

"Contactless"

"Dual Interface"

Why are EMV transactions considered more secure?

- Data on the transaction generated by the chip authenticates the card to the issuer.
- EMV transactions may also include a PIN which authenticates the cardholder to help prevent fraud through lost or stolen cards.
- The microprocessor chip creates a unique transaction code that cannot be used again each time an EMV card is used for payment. If a hacker attempted using stolen chip information from a specific point of sale, the stolen transaction number created in that instance wouldn't be useable again and the transaction would be denied.

Secure Elements of an EMV Transaction

The EMV Transaction:

1. EMV terminal prompts EMV card to be inserted. EMV chip application performs risk assessment.
2. Primary Account Number (PAN) and Dynamic Card Verification Value (CVV) are used in the authorization.
3. Dynamic CVV is validated against what's expected at issuer host.

EMV Liability Shift

- October 2015 Liability Shift: The party responsible for a chip transaction not occurring will be financially liable for any resulting card present counterfeit fraud losses. TransFirst will enable EMV contact and contactless processing for all card types.

Visa®	MasterCard®	American Express®	Discover®
• EMV must be enabled	• EMV must be enabled • Must support both contact and contactless interfaces	• EMV must be enabled	• EMV must be enabled • Must support both contact and contactless interfaces

- The liability shift encompasses all face-to-face transactions, including cash advance.

U.S. Migration Progress

- April 2013:TransFirst EMV® deployment capabilities are underway.
- Merchants are beginning to invest in hardware upgrades to accept EMV chip cards.
- ATM providers are actively deploying EMV-enabled ATMs.
- According to Visa, of the 1 billion+ cards that are in use in the U.S., roughly 117 million EMV cards have been issued in the U.S. collaborating with the EMV Migration Forum reports that the U.S. payments industry is on track to see 100 million or more EMV chip cards issued

What EMV Will Require

- An upgrade to the systems used by issuers, acquirers and processors for payment processing (largely complete)
- An upgrade of the merchant's point-of-sale (POS) environment, including both hardware and software
- A change in the traditional process consumers use to make a purchase edit or debit cards

What EMV is Not

- EMV is **not** a “silver bullet” for PCI compliance and account data compromise protection.
- EMV is **not** a cure-all for chargebacks.
  - The programs put in place by the associations will help reduce incidents of counterfeit card related fraudulent chargebacks, but will not reduce or impact reasons for other chargebacks.

Counterfeit Chargeback Codes

EMV reduces the potential for the following chargeback codes:

Visa®

- # **62**: Counterfeit
- # **81**: Fraud Card Present
- # **93**: Fraud – Merchant Performance

MasterCard®

- # **4840**: Fraudulent Processing of Transaction
- # **4870**: Chip Liability Shift
- # **4871**: Chip/PIN Liability Shift

Additional Considerations for Businesses

- What type of merchandise do you sell or services do you provide?
- How well do you know your customer? Do you have an ongoing relationship with them?
- Do you have one or more locations in geographic markets where banks have begun issuing chip cards to their cardholders?
- How many counterfeit chargebacks do you receive each year?
- What type of point-of-sale (POS) system do you have?

Implementation Options

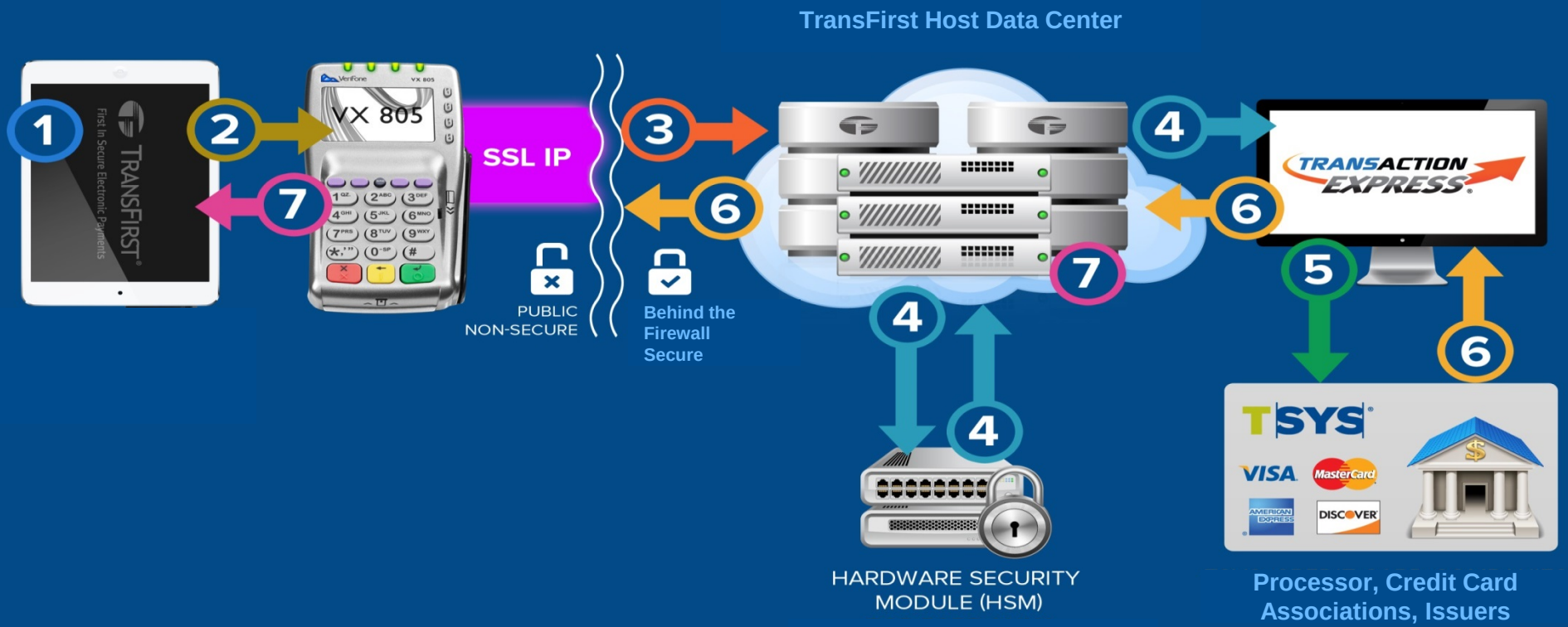
- For Countertop and Wireless Terminals – Simple Implementation Option

  1. Buy a new terminal
  2. Download it with the EMV capable application
  3. Follow the prompts on the terminal to complete a transaction

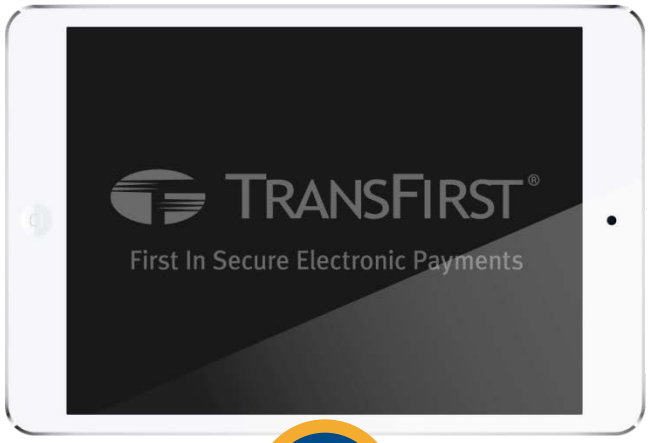
- For Complex, Integrated POS Solutions

  — Semi-Integrated Processing Option

SEMI-INTEGRATED TRANSACTION FLOW WITH EMV AND NFC CAPABILITY



In the Semi-Integrated Transaction Flow model, the software does not process the card data itself. The ProcessNow® Register / Other VAR POS Software App works with a peripheral "super PIN pad", the VeriFone VX 805, for traditional magnetic stripe swiping, or EMV chip slot, or NFC tap-and-go payment processing, or by key entering card data into the key pad. The VX 805 is a secure, hardened device that also has an optional P2PE encrypting capability.



Step 1

Ring up order in the POS Software

2

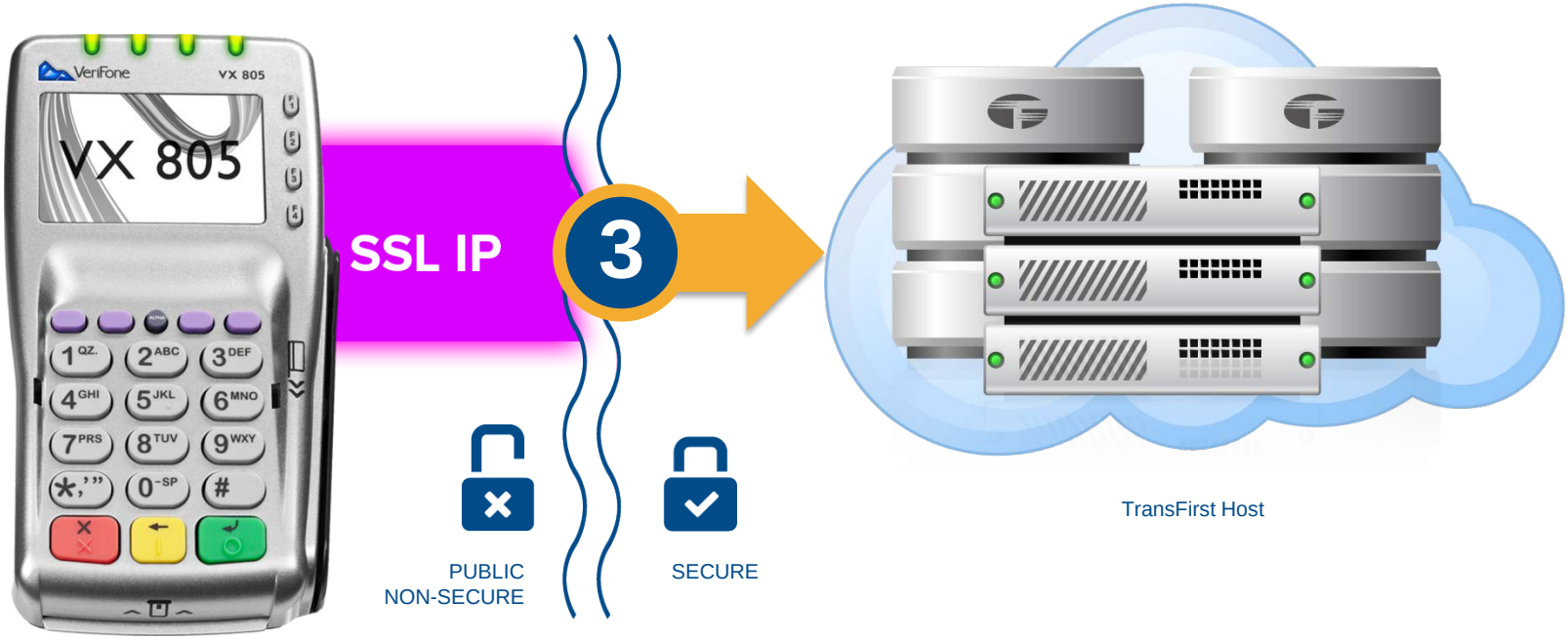
Step 2

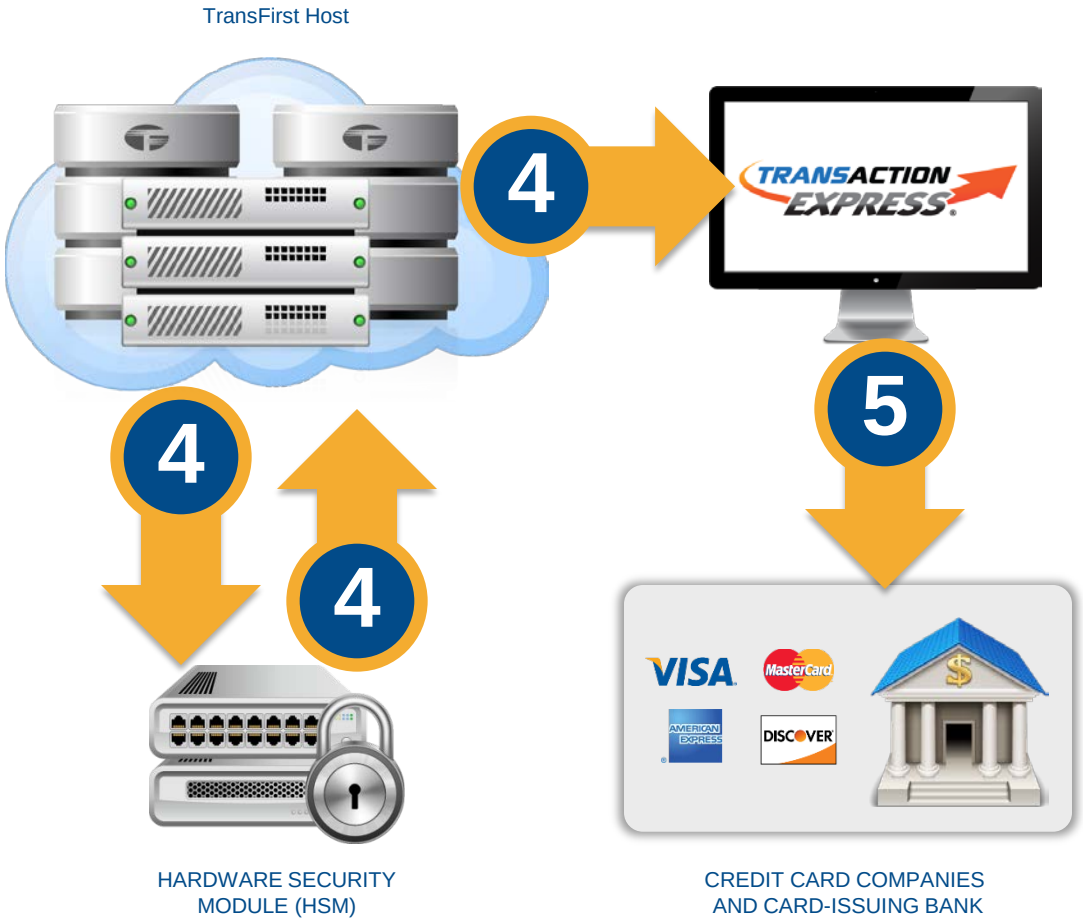
Press credit/debit tender option to send the dollar amount of the payment request to a peripheral “super PIN pad” device

Step 3

The peripheral device captures card payment data and sends secure data information to the information to your acquirer/processor directly.

» By chip card insertion into the EMV internal chip slot;
» Or by tap-and-go using NFC;
» Or by swiping traditional magnetic stripe cards;
» Or by key entering card data into the key pad on the VX 805.
» P2PE may be incorporated in this solution
» Tokenization may be incorporated into this solution



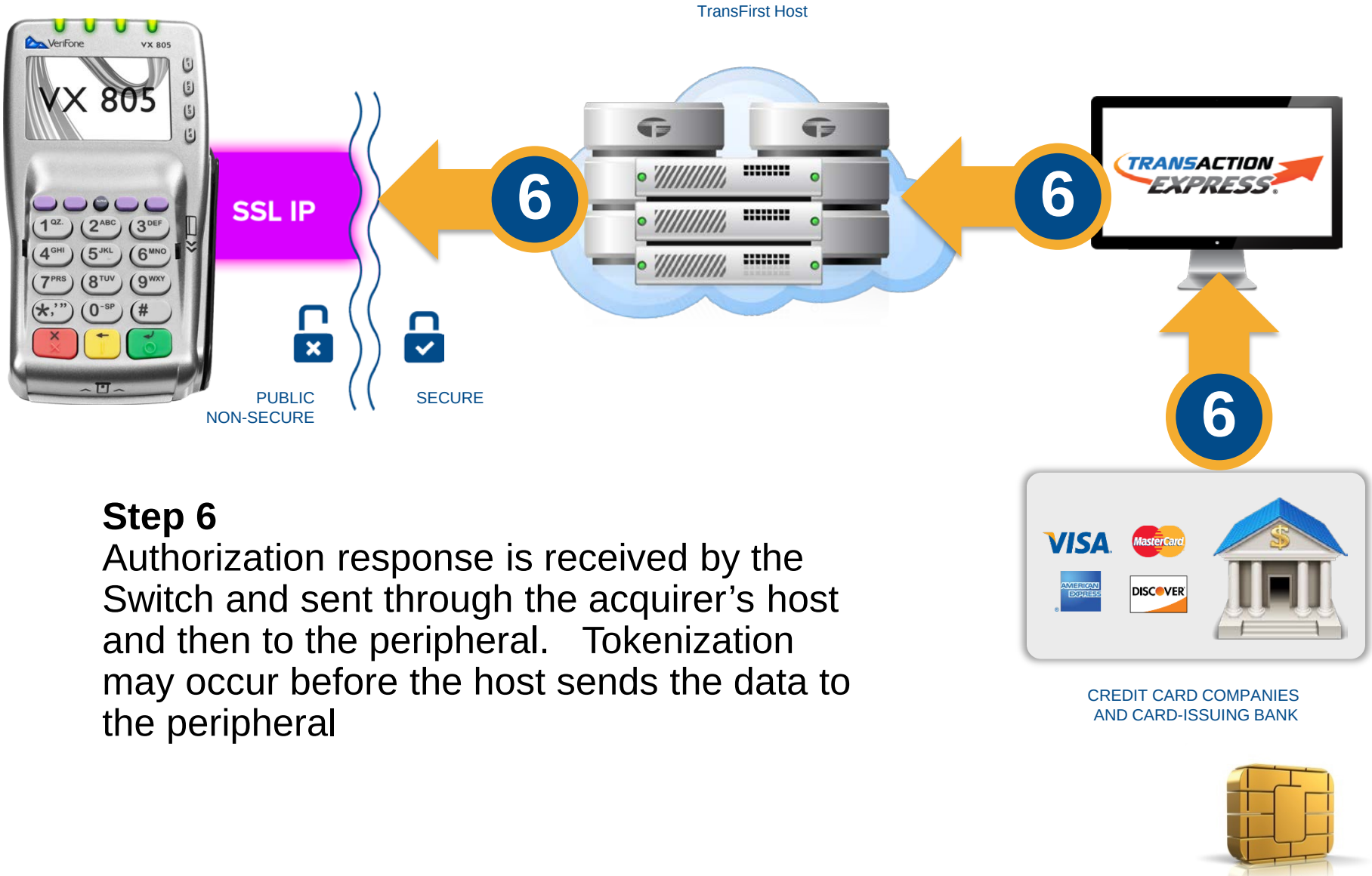


Step 4

The Acquirer's host then sends the secure encrypted data to a switch (Transaction Express®) for processing. **If P2PE or PIN Translation is involved**, the encrypted data is sent to Hardware Security Module (HSM) for safe decryption and clear text message creation, re-encryption of the PIN Block prior to being sent to the switch.

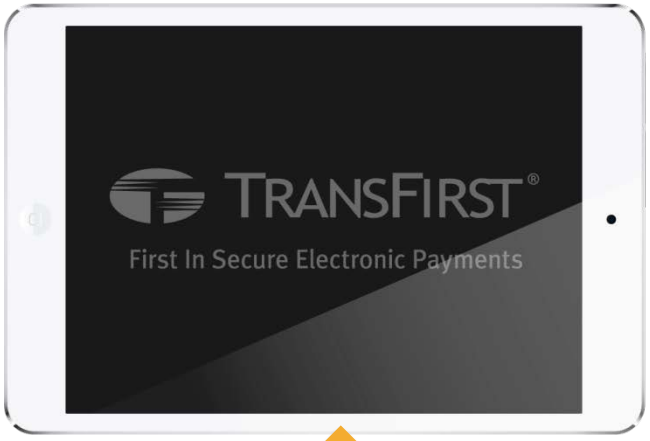
Step 5

Transaction is processed via normal paths (Switch to Processor, Credit Card Companies / Card-Issuing Bank).



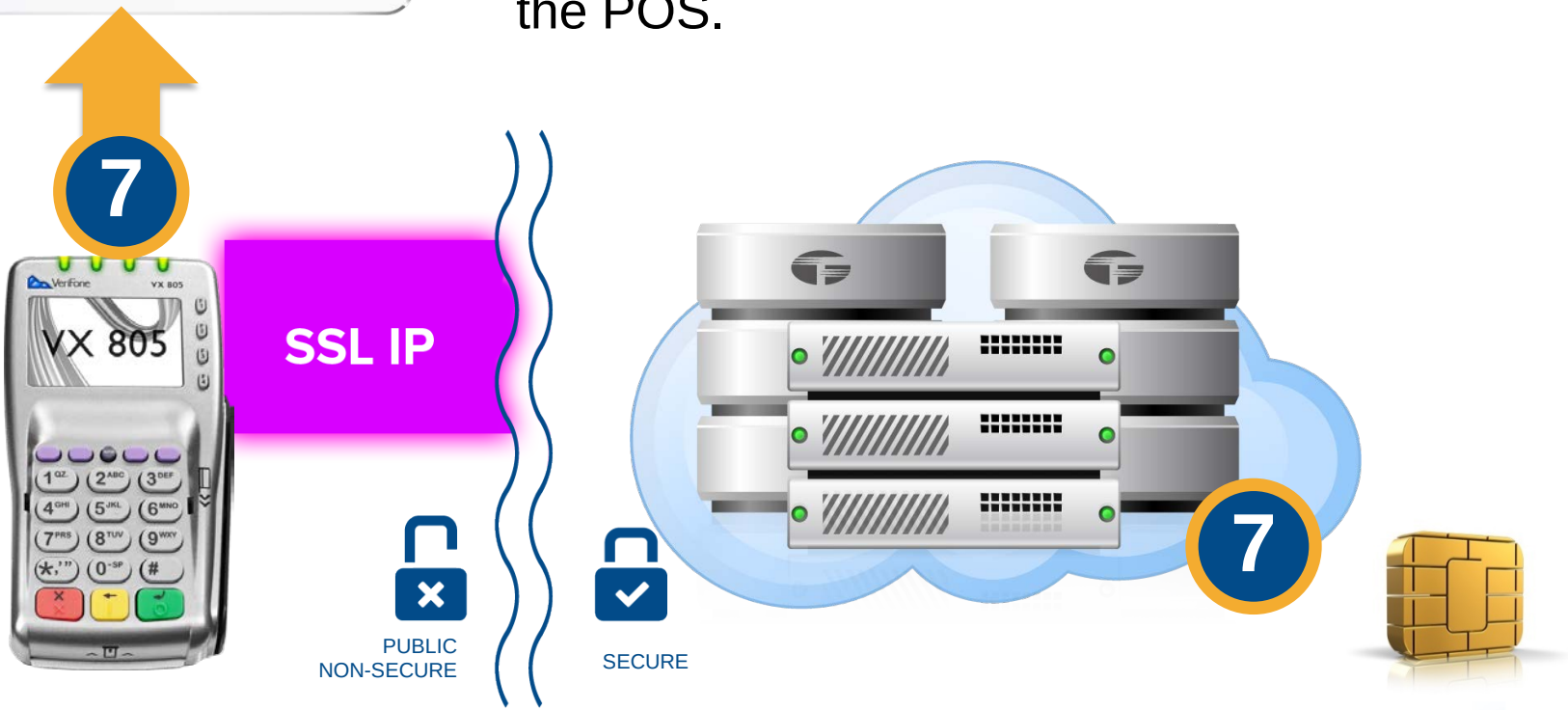
Step 6

Authorization response is received by the Switch and sent through the acquirer's host and then to the peripheral. Tokenization may occur before the host sends the data to the peripheral



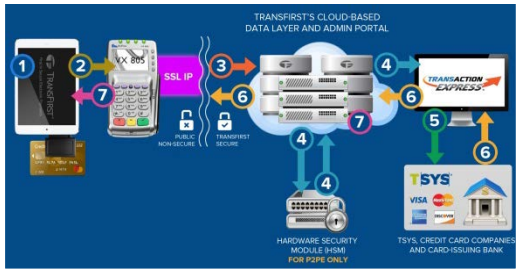
Step 7

Truncated payment data is sent from the Peripheral to the POS to complete the transaction. Full transaction data should be stored only acquirer's host. Tokens may be sent with the truncated data to the POS.



What are the benefits of the Semi-Integrated Model?

Semi-Integrated Model



- Has the potential to eliminate the need for PA DSS.
  - Offers the largest reduction on PCI scope of the point-of-sale software.
- Card-swiped and key-entered transactions are both secure.
- The peripheral is a hardened, locked down, secure device.
  - P2PE becomes less material.
- EMV Certification of the VAR software can be eliminated because it is the peripheral that is EMV certified and in communication with the acquirer's host.
  - The value to the software VAR is enormous.

EMV Implementation Steps

1. Learn by gathering EMV information from EMVCo, the card brands and the TransFirst.com Learning Center — an excellent free resource for information on the latest developments in electronic payment processing.
2. Plan your implementation.
   - Identify your project team – dedicated resources
   - Review the devices used by your card present merchant base
   - Decide how you want to implement
3. Gather requirements, define objectives, set goals and timelines.
   - Take the project in steps vs. tackling the entire initiative at once
   - Gain successes, momentum, and believers
4. Test (internal and external), activate with your processor and deploy a pilot prior to rollout.

Questions?

TRANSFIRST®
First In Secure Electronic Payments

We Can Help!

TRANSFIRST®

First In Secure Electronic Payments

Contact Us

800-613-0148

www.TransFirst.com

EMV is a registered trademark in the United States and other countries, and is an unregistered trademark in other countries, owned by EMVCo. Other trademarks are property of their registered owners and are not necessarily affiliated with TransFirst. All accounts subject to credit approval; some restrictions and exclusions apply to all offerings. TransFirst, LLC is a registered ISO/MSP of: Wells Fargo Bank, N.A., Walnut Creek, CA, and Synovus Bank, Columbus, GA, for Visa and MasterCard transactions only.