Encryption and Tokenization: Protecting Customer Data

Tia D. Ilori
Sue Zloth
September 18, 2013

Agenda

- Global Threat Landscape
- Real Cost of a Data Breach
- Evolution of Point-to-Point Encryption and Tokenization
- Visa Merchant Data Secure

Visa Global Security Summit

The Visa Global Security Summit is a must-attend event for executives from business, government, academia and law enforcement. The conference will explore the intersection of technology and security, and participants will offer diverse perspectives on how industry and government can collaborate to address cyber security issues.

- Pre-Summit Risk workshops for acquirers, merchants, and processors: Oct 1st
- General Session: Oct 2nd

Register at: http://www.VisaSecuritySummit.com

Visa's Multi-Layered Strategy

Mitigating fraud through continuous leadership, coordination and investment

- Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid

PCI DSS Requirements

Commonly Identified Security Deficiencies

	Vulnerability	Applicable Requirement
Network Security	Default or no firewall / router rules	Requirement 1
	No DMZ	Requirement 1
	Insecure remote access, no 2-factor authentication	Requirement 8
Host-based Security	Insecure operating systems and databases	Requirement 6
	No patching	Requirement 6
	No or outdated anti-virus signatures	Requirement 5
	No password management or access control lists (ACL)	Requirement 7
	Use of default or shared usernames and passwords	Requirement 2
	No system logging	Requirement 10
	No file integrity monitoring	Requirement 10
Application Security	SQL injection / other web-based exploits	Requirement 6
	No secure coding, independent code review, or penetration testing process in place	Requirement 6
Incident Response	No incident response plan	Requirement 12
General	No monitoring of systems, logs, access control, etc.	Requirement 10

- **Lack of network segmentation has contributed to multiple location breaches**

Source: Data breach forensic reports

Data Security Best Practices

- Implement PCI DSS, including a PA-DSS compliant application
- Secure remote access connectivity by IP address (or disable if not necessary)
- Use 2-factor authentication
- Use strong passwords when accessing POS systems
- Implement a hardware-based stateful firewall and enable filtering for inbound and outbound traffic
- Enable logging on systems and periodically monitor for malicious activities
- Do not use your POS systems to browse the Internet, email, etc.
- Ensure POS systems have latest anti-virus signature files
- Remove unnecessary accounts/services on POS systems
- Enforce data security on third-parties via contracts
- Enroll in a managed firewall and vulnerability scan program

Real Cost of a Data Breach

- Data breaches impacts your company's bottom line
- Average cost of a data breach was $136 a record
  - $188 in the U.S.
- Average number of breached records was 23,647
  - 28,765 in the U.S.
- U.S. organizations spent on average $565,020 on notification costs
- Root cause of U.S. breaches
  - Malicious or criminal attack – 41%
  - Human factor – 33%
  - System glitch – 26%

Source: Ponemon/Symantec 2013 Cost of Data Breach Study

Poll Question #1

What payment security issues keep you up at night?

- Is my data secure?
- Has my payment environment been breached?
- What can I do to protect my data from hackers?
- All of the above

Point-to-Point Encryption and Tokenization – how did we get here?

Major Breaches

- **TJ Maxx, 2007:** In the first major breach, hackers embedded malware onto an internal network stealing 46 MM cards
- **Heartland, 2009:** A multi-month malware intrusion compromised information for nearly 100 MM payment cards
- **Global Payments, 2012:** International hackers embedded malware to capture 1 MM payment cards, and PII data

Increased Vigilance

- **Visa released guidance docs – Encryption in 2009 and Tokenization in 2010**
- **PCI SSC released guidance docs – Encryption in 2010 and Tokenization in 2011**

Encryption Market Today

- **Many solution providers offer products**
- **Lack of clarity for leading industry practices**
- **Visa continues leading PCI SSC and the industry in development of standards and solutions**

Sources: Bloomberg Business Week, BankInfo Security, The Boston Globe

Transaction Flow

Point-to-Point Encryption

1. POS Transaction

Original Card Number:
4000123456789010

2. Data Encryption

Encrypted Card Number:
4000129999999010

3. Leading Security

Decrypted Card Number:
4000123456789010

Tokenization

4. Return Token

Card Token:
4123456789101112

5. Secure Transmission

Card Token:
4123456789101112

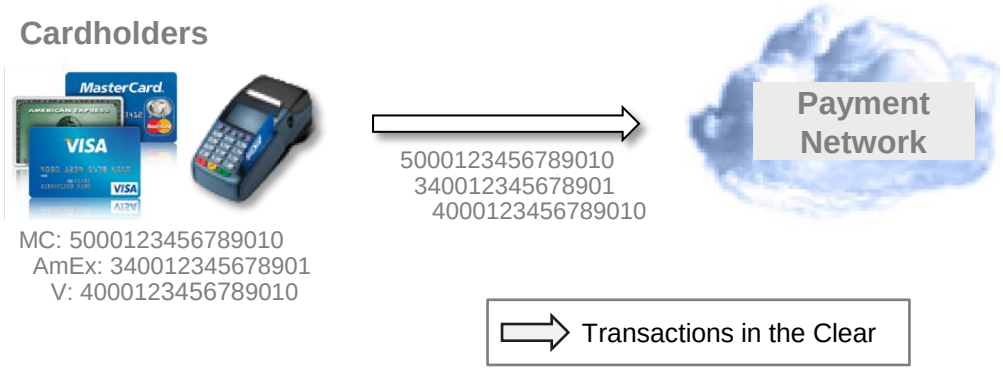
6. Safe Storage

Stored Value:
4123456789101112

EMV and Point-to-Point Encryption

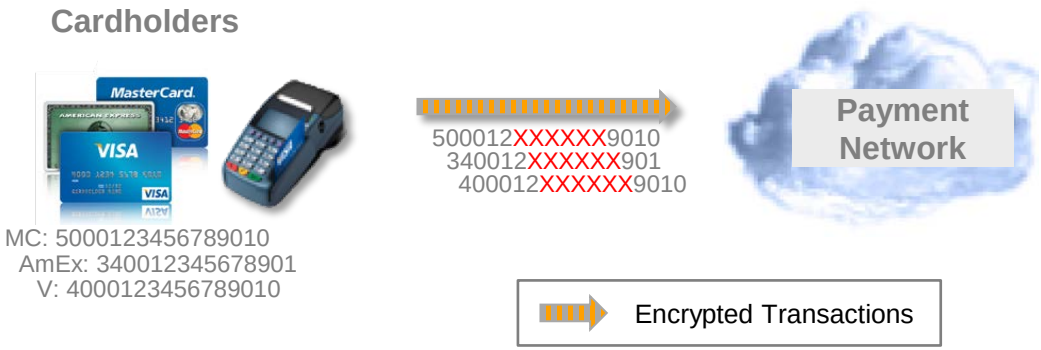
EMV Only

- Dynamic authentication
- Account number and card data remain exposed
- Exposure of sensitive information results in cross-channel fraud



EMV and Encrypted Transactions

- Dynamic authentication
- Account number and card data **are protected in transit**
- Strongly mitigates the risk of point-of-sale and cross-channel fraud



PCI SSC and P2PE/Tokenization

P2PE

- PCI has introduced a validation program for Point-to-Point Encryption
- Merchants who use a validated P2PE Solution may qualify for scope reduction
- 2013 and 2014 releases will likely focus on hybrid (aka software) encryption

Tokenization

- In addition to the Guidance previously released, PCI SSC has started to look at Tokenization Standards and Requirements

See the PCI website at https://www.pcisecuritystandards.org for more information

Technology solutions – who could they help in securing payment data?

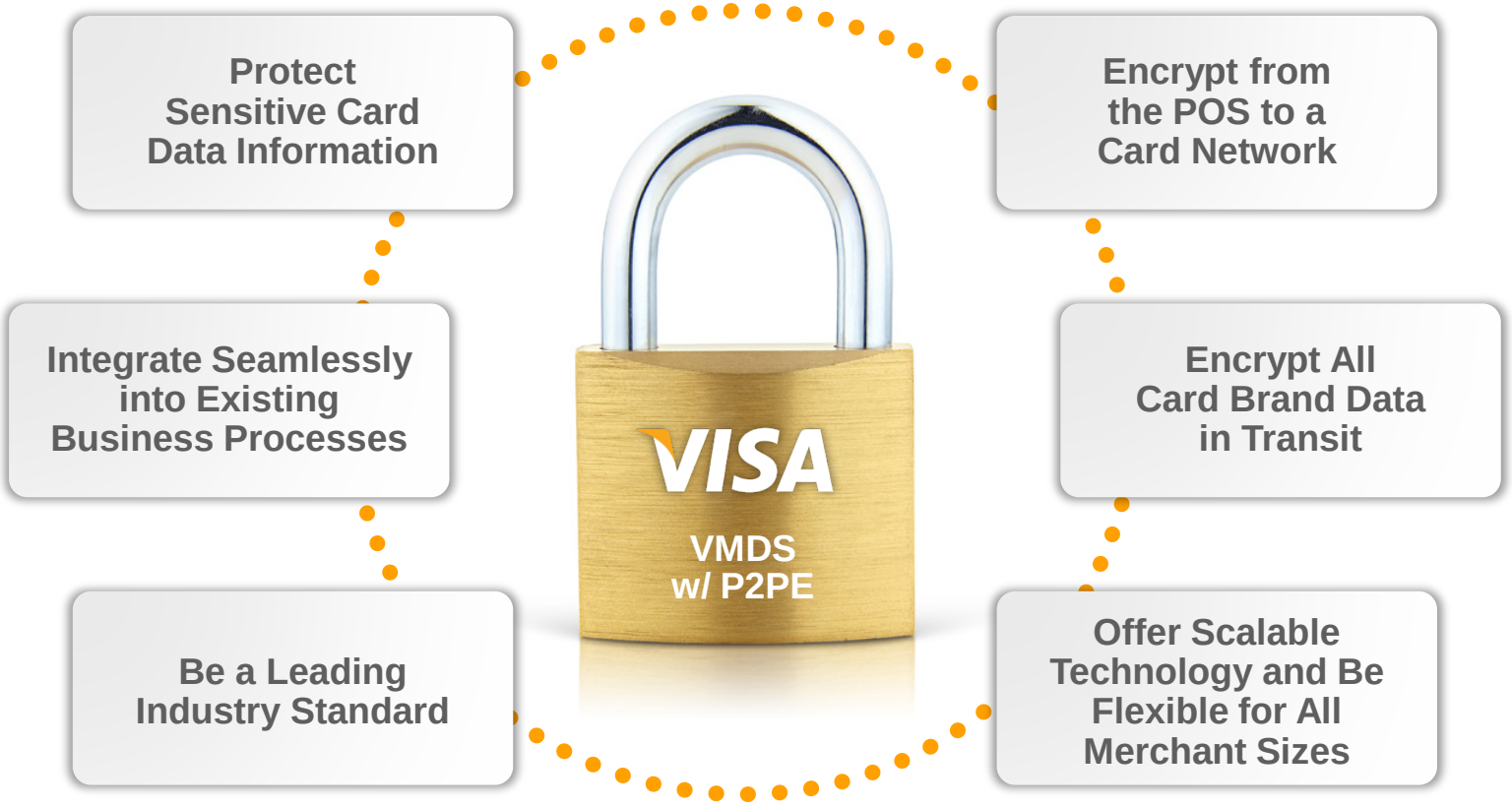
	Brick and Mortar Merchant	E-Commerce Merchant	Service Provider
Hardware Encryption	✓		✓
Software Encryption	✓	✓	✓
Tokenization	✓	✓	✓

Poll Question #2

Have you implemented a P2PE solution? If not, are you looking at one?

- Yes, and it works well
- Yes, but we're looking for an alternative
- No, but we're interested
- No, and we're not interested

Visa Merchant Data Secure with Point-to-Point Encryption (VMDS with P2PE) Is Being Developed to:



Proposed service in development and presented for discussion purposes only; service functionality, features and timelines subject to change by Visa at any time.

Visa Merchant Data Secure Product Features

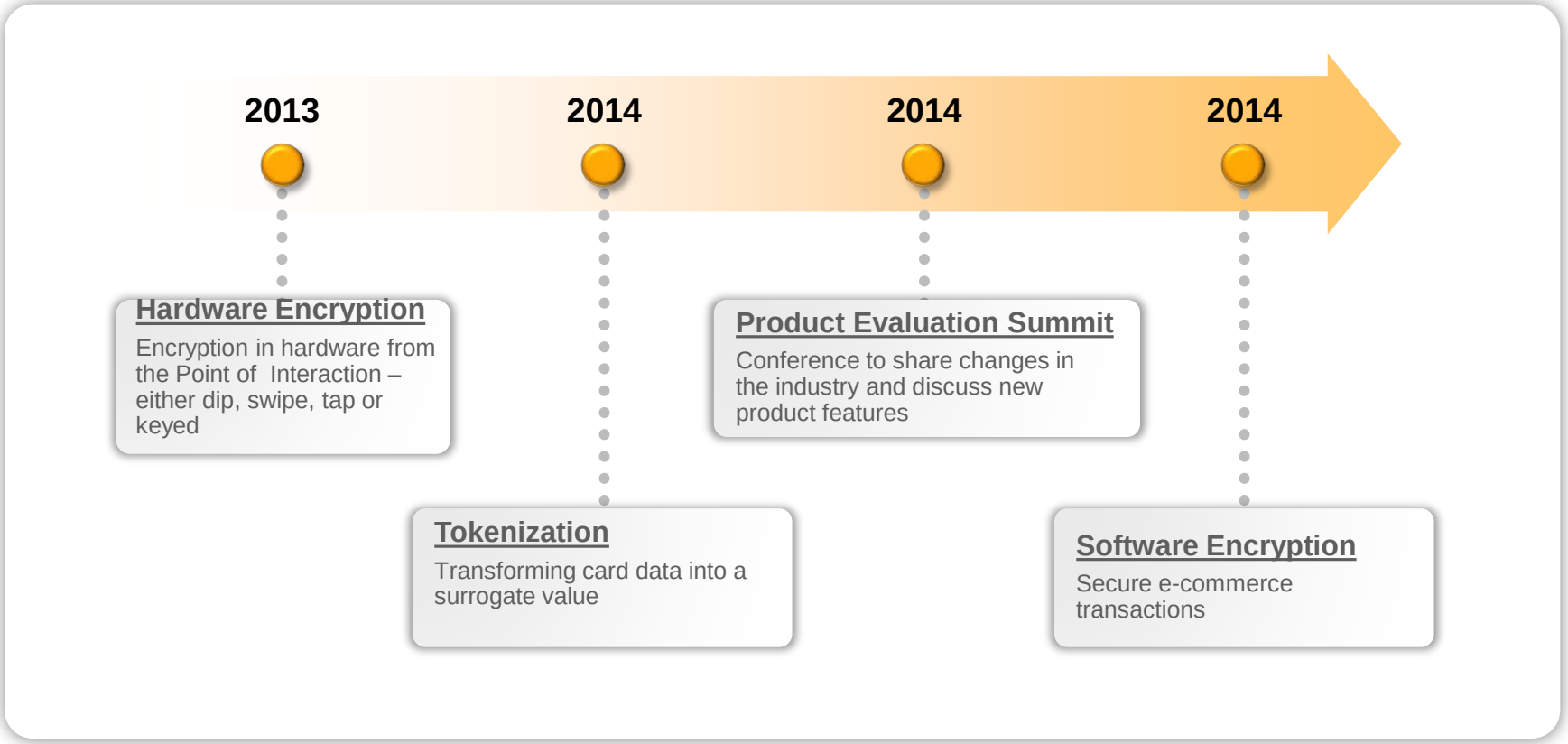
	VISA Merchant Data Secure
Hardware Encryption	✓
Single Key Injection	✓
Zone Translation	✓
Standards-based (TDES + DUKPT)	✓

Use of zone translation and standards-based technology enables VMDS w/P2PE to become an industry standard for encryption

Proposed service in development and presented for discussion purposes only; service functionality, features and timelines subject to change by Visa at any time.

Roadmap for Development

Visa Plans to Expand the VMDS Product Suite by Providing Customers with Solutions for Enterprise Security



Proposed service in development and presented for discussion purposes only; service functionality, features and timelines subject to change by Visa at any time.

Visa Global Security Summit

The Visa Global Security Summit is a must-attend event for executives from business, government, academia and law enforcement. The conference will explore the intersection of technology and security, and participants will offer diverse perspectives on how industry and government can collaborate to address cyber security issues.

- Pre-Summit Risk workshops for acquirers, merchants, and processors: Oct 1st
- General Session: Oct 2nd

Register at: http://www.VisaSecuritySummit.com

PCI SSC Community Meeting

- PCI Security Standards Council (SSC) North America Community Meeting
- September 24-26, 2013
- Las Vegas, Nevada
- Visa will host “office hours” throughout the community meeting
  - Participating organization are encouraged to take advantage of this unique opportunity to engage with Visa representatives
  - For more information please visit https://www.pcisecuritystandards.org/communitymeeting/2013/north-america

Questions

For More Information Please Contact:

Sue Zloth
mds@visa.com
www.visamerchantdatasecure.com

Tia D. Ilori
cisp@visa.com
www.visa.com/cisp