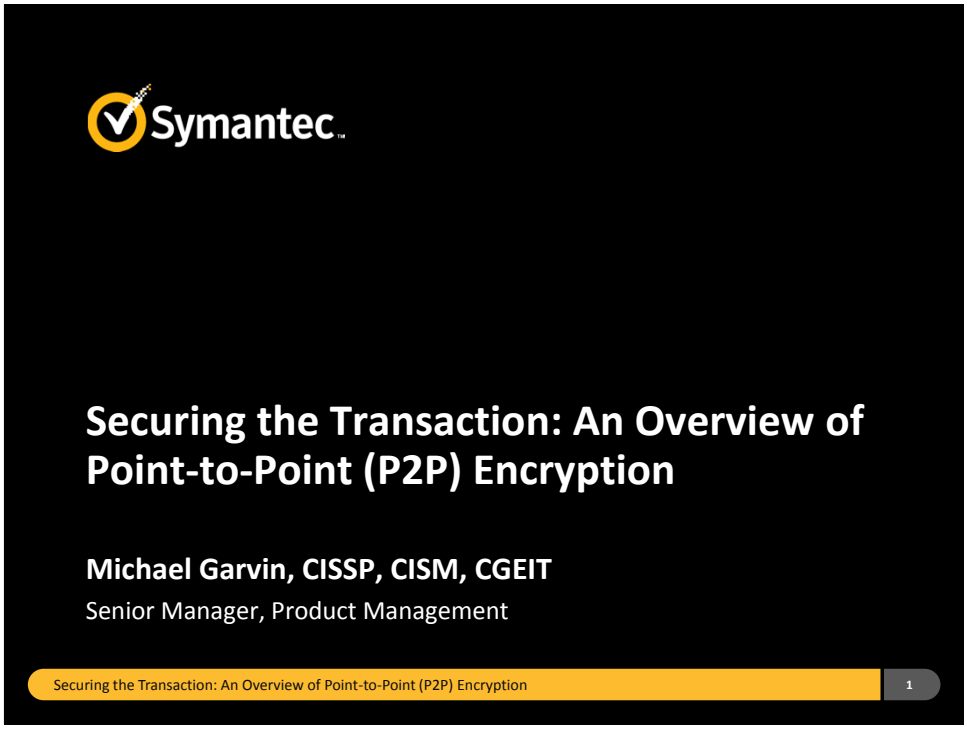
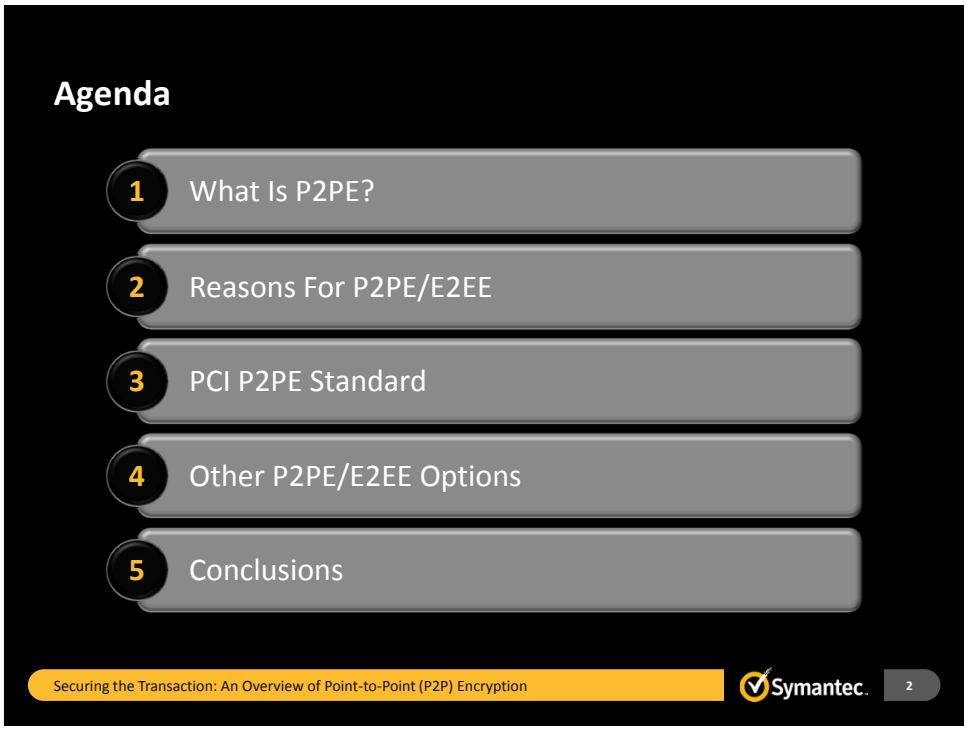

Symantec.
Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption
Michael Garvin, CISSP, CISM, CGEIT
Senior Manager, Product Management
Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption
1


Agenda
1 What Is P2PE?
2 Reasons For P2PE/E2EE
3 PCI P2PE Standard
4 Other P2PE/E2EE Options
5 Conclusions
Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption
Symantec.
2

What Is P2PE?

- Point-to-Point Encryption; may also be known as End-to-end Encryption (E2EE)
- A way to reduce – not eliminate – scope for PCI DSS compliance and assessment
  - Also to increase security, and to reduce risk and liability
- PCI has the P2PE Standard
- As with all things PCI, "it depends"

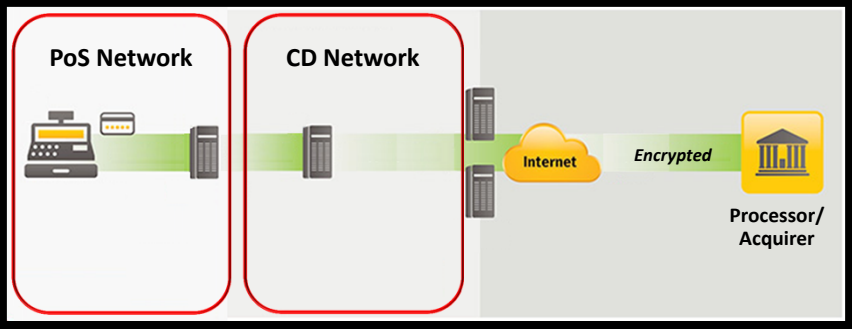
PCI DSS and Terminology Refresher

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

- PAN, SAD, CHD, and CDE (oh my!)

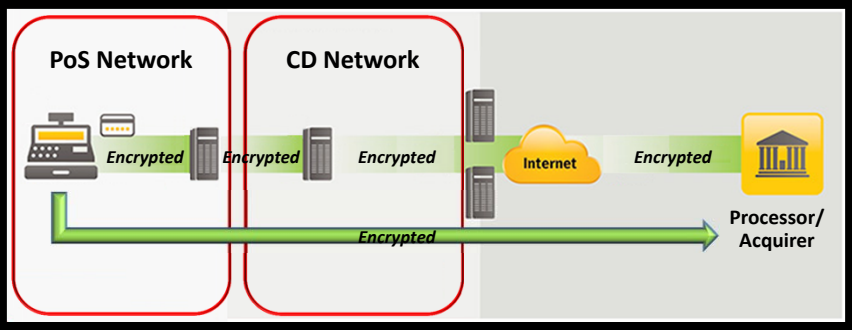
Reasons For P2PE/E2EE

Typical Implementation Before P2PE/E2EE



- Segmentation into "zones of trust" with varying data security
- Scope for compliance and assessment may not be minimized
- Likewise, neither may security and business risk

Implementation With P2PE/E2EE



- Encrypted data flows through existing channels, or is sent directly to a service provider
- Organization has limited/no ability to decrypt cardholder data
- Scope is limited, risks are reduced

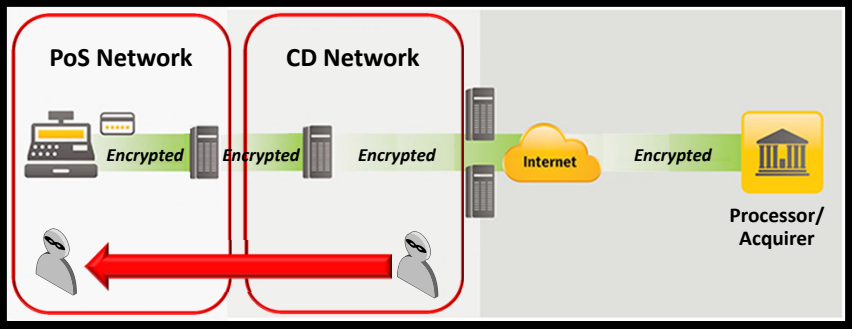
PCI P2PE Standard

PCI P2PE Terminology

- PCI P2PE Standard
- PTS – PIN Transaction Security (PCI standard)

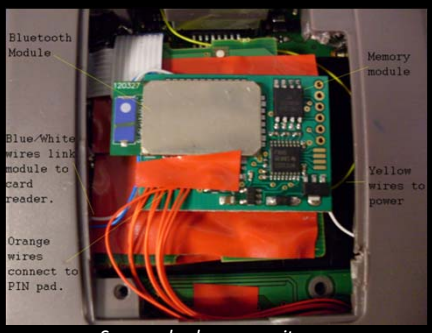
- POI – Point of Interaction (for P2PE, evaluated and approved via the PCI PTS program, with SRED listed, enabled and active)
- SRED – Secure Reading and Exchange of Data (PTS module defining POI device security requirements)
- HSM – Hardware/Host Security Module (protected hardware device that provides a secure set of cryptographic services)
- SCD – Secure Cryptographic Device (implements cryptographic logic or processes)

Shifting Security, Risks With P2PE



- Limit access to cardholder data (stored and transmitted; processed?)
- Transfer responsibility from the organization
- Risks may move closer to the POI, or to POI infrastructure

Physical Terminal Attack



Source: krebsonsecurity.com

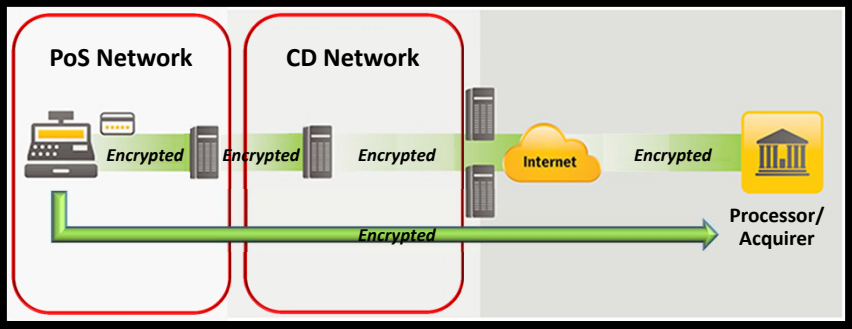
- Modification of hardware to capture or duplicate card data
  - Eg, the Aldi attacks
- Physical security and employee awareness is still critical

A High Bar

- Requires PTS and SRED compliant POI's, P2PE compliant solutions and applications
  - Possible rip-and-replace
  - Cost/benefit versus PCI DSS operations
  - Currently 3 solutions and 3 applications certified
- Service providers are in scope, and selection must be considered carefully
  - Assessment status, third party risk, liability, etc.
- Requires assessment and validation
- Subject to many of the same issues as PCI DSS compliance (people and processes, on top of technology)

Other P2PE/E2EE Options

Implementation With P2PE/E2EE



- Limit access – encrypt data, separate duties, and segment
- Consider impacts on security, compliance, and assessment
- Scope is limited, risks are reduced, cost may be reduced

Conclusions

Conclusions

- Consider the end game – business goals, security, compliance, risk, liability, etc.
- P2PE requires PTS and SRED compliant POI's, P2PE standard compliant solutions and applications
  - Possible rip-and-replace; cost/benefit versus PCI DSS operations
  - Currently 3 solutions and 3 applications certified
- E2EE and/or principles implemented within the CDE may achieve some of the same goals
- Third parties are in scope, and selection must be considered carefully
  - Assessment status, third party risk, liability, etc.
- Issues as PCI DSS compliance come into play (people and processes, on top of technology)


Symantec
Thank you!
Michael Garvin, CISSP, CISM, CGEIT
Senior Manager, Product Management
michael_garvin@symantec.com
Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.
Securing the Transaction: An Overview of Point-to-Point (P2P) Encryption
17