The PCI Security Standards Council
PIN Transaction Security Program Updates: PTS 3.1 and
PCI PIN Security Requirements 1.0

Leon Fell
Director of Solution Standards
November 2011
Agenda

- Introduction
- The Foundation to Build Upon
- POI Security Requirements v3.1
- PIN Security Requirements v1.0
- What’s Next
- Open Mic
About the Council

Open, global forum

Founded 2006

Responsible for PCI Security Standards

- Development
- Management
- Education
- Awareness
PCI Security Standards

Payment Card Industry Security Standards
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users
**PTS Lifecycle**

**Major new release of PTS**
- Presented at Community Meetings
- Initiates 3-year lifecycle

**PTS Errata**
- The Council may publish errata at any time if so required
- If errata are required, they usually will become effective immediately
Agenda

- Introduction
- The Foundation to Build Upon
- POI Security Requirements v3.1
- PIN Security Requirements v1.0
- What’s Next
- Open Mic
PCI PTS Program 2010

PCI PTS Device Program

Point of Interaction (POI) Devices

Hardware Security Modules (HSMs)

Logical and/or physical protection of cardholder and other sensitive data
Where We Have Been

Program consolidation

Secure Reading and Exchange of Data

PCI PTS POI Security Requirements

MasterCard PTS

PCI PTS

Open Protocols

PCI UPT

PCI EPP

PCI POS PED
# PTS – 2010 New Modules

<table>
<thead>
<tr>
<th>Open Protocols</th>
<th>Ensures that open protocols in POIs do not have vulnerabilities that can be remotely exploited and yield access to sensitive data or resources in the device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Covers IP connectivity (internet), GPRS, Wi-Fi</td>
</tr>
<tr>
<td>Secure Reading and Exchange of Data (SRED)</td>
<td>Enables cardholder data to be secured or protected (i.e. truncation) after being read by the PTS terminal; it then enables the secured cardholder data to be transmitted from the terminal</td>
</tr>
<tr>
<td></td>
<td>Secure foundation for Point to Point encryption</td>
</tr>
<tr>
<td>Integration</td>
<td>Ensures integration of previously approved components does not impair the overall security as stated in security requirements</td>
</tr>
<tr>
<td></td>
<td>Supports the cost-effective maintenance of components</td>
</tr>
</tbody>
</table>
Agenda

- Introduction
- The Foundation to Build Upon
- POI Security Requirements v3.1
- PIN Security Requirements v1.0
- What’s Next
- Open Mic
POI Security Requirements V3.1

Errata

• Standard 12-18 months after initial publication

P2P Support – Leverage Existing POI Criteria

• Secure (Encrypting) Card Readers
  – Select Core and SRED Requirements

• Non-PIN Entry Devices
  – Mandatory SRED module
  – Open Protocols (if applicable)
PTS Security Requirements v 3.1

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

Modular Security Requirements
Version 3.1
October 2011
PTS POI Secure Card Readers (SCRs)

New Approval Class – Secure (Encrypting) Card Readers

Form Factor

- OEM (integrates)
- Stand-alone (e.g., USB attached)
- ICCR, MSR, Hybrid

Meets specific POI criteria

- Select Core and SRED Requirements
- Both physical and logical

Lab validates reader and possible integration into a POI device

QSA validates implementation in a PCI P2PE validated solution
Mobile Phone Plug-in MSR

- Audio connector plugs into the phone’s headphone jack.
- Also works on computers – any device with an audio input jack.
- Plug-in MSR encrypts data on the reader even before it reaches the phone.
- Again – QSA must determine data NOT decrypted on phone.
- No PIN entry.

Also works on computers – any device with an audio input jack.
### Mobile Guidance for PTS PEDs

**Dual Purpose Device**

- PED and Phone integrated into single tamper protected device
- Physically and logically hardened in accordance with the PTS POI security requirements.

**Handheld PED designed to accommodate attachment of phone**

- Dual sided
  - Phone
  - PED keypad
- PED must be SRED approved
- PED must also control the card reader(s)*

*NOTE in scenario 2 the data must be devalued by not allowing capture of both PIN (inadvertent entry on the non-secure interface i.e., the phone) and account data (phone never sees clear account data)
PTS PED Vendor Solutions – Scenario 1

Phone is designed and purpose built as a secure device

By definition does not use off the shelf mobile phones

Because secure tamper protected device, may use either SCR or a data key managed similar to PIN key
PTS PED Vendor Solutions – Scenario 2

- Cradle for phone
- Card readers integrated to PED
- May employ encrypting card reader or use data key managed similar to PIN key
Company
XYZ

Approval Number
4-10102

Version
3.X

Product Type
SCR

Expiry Date
30, April 2020

Approval Class
SCR

Functions Provided
ICCR, MSR

PTS SCR Approval Listing - Example
Non-PIN Entry Devices

New Approval Class – Non-PEDs

Evaluation Criteria

- Secure Reading and Exchange of Data (SRED) Module
- Open Protocols Module (if supports)

Separate list from PIN acceptance devices

Functions Provided

- SRED
- OP
PTS POI V2 Devices

**Parameters**
- Twelve month window
- Expiration remains April 2017

**Validation**
- SRED module (mandatory)
- Open Protocols (if applicable)

**Functions Provided**
- SRED
- OP
May leverage requirements that it previously met in v2 where those requirements parallel SRED requirements

- May utilize algorithms and key sizes allowed in v2 in lieu of those specified in SRED
- May utilize v2 attack potential calculations for SRED requirements previously addressed under v2

V2 devices “upgraded” using encrypting card readers must meet not only SRED, but the applicable card reader requirements in the Core section (the same as is done for approving card readers under v3.1)
Categories of PTS POI Products

- **Attended POI PIN Entry Terminals/Non-PEDs**
- **OEM Components:** EPP, PED, SCR
- **Unattended Integrated POI Terminals**
Applying the Products to the Flow Chart
Agenda

Introduction

The Foundation to Build Upon

POI Security Requirements v3.1

PIN Security Requirements v1.0

What’s Next

Open Mic
The New PIN Transaction Security Umbrella

PIN Transaction Security

Point of Interaction

Hardware Security Module (HSM)

PIN Security
Core Principles

Dual Control

A process of using two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person must be able to access or to use the materials (e.g., cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of the key among the entities.

Split Knowledge

A condition under which two or more entities separately have key components that individually convey no knowledge of the resultant cryptographic key.
Seven Control Objectives

Secure Equipment and Methodologies

Key Generation (unpredictable)

Key Conveyance

Key Loading

Key Usage

Key Administration

Equipment Management
Secure Equipment and Methodologies

- PINs processed in SCDs
  - Newly deployed POIs must be PCI approved
  - Newly deployed HSMs recommended
  - Stipulate in P.O.

- Approved algorithms
  - TDES
  - RSA

- Secure PIN blocks

- No logging!
Key Generation

- Pseudo-random process
- Dual control - collusion
- Split Knowledge
- Secure key formation
- Documentation
Key Conveyance

- Different channels
- Tamper evident authenticable packaging
- Cipher text
- Equivalent or greater strength
- Authorized custodian
- Documentation
Key Loading

Multiple components/cryptogram

Public key (Annex A)

Dual control – KLDs

Protect against monitoring

Validation

Documentation

Dual control

Split Knowledge
Key Usage

- KEK/PEK
- Production/Test
- Unique host to host
- Unique per device
- Unique per intended use
Key Administration

Allowed Key Forms

SCD

Components

Cryptograms

Compromise

Destruction

Authorized Custodians

Logs

Removal from storage

Loading

Documentation
Management of Cryptographic Equipment

- Placing into service
  - Unauthorized modifications/substitutions

- Removal from service
  - Remove all secret data
  - Destroy where necessary

- Dual Control operations
  - KLDs
  - HSM configurations

- Documentation
Normative Annex A

Symmetric Key Distribution Using Asymmetric Techniques

- Same Control Objectives and the applicable requirements as the main body of the PIN Security Requirements
- Provides specific additional criteria for entities implementing automated remote key distribution using asymmetric cryptographic algorithms
- Two distinct areas
  - Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations
  - Characteristics of the actual key-distribution methodology implemented
Key Concepts

CA/RA Operations – New Principles

• Trustworthy Systems
• Level of Assurance

Mutual Authentication

• Man-in-the-middle
• POI must provide a way to ensure the validity of the host involved in the communication prior to any:
  – Key transport
  – Key exchange
  – Key establishment

• Replay attacks
• Make infeasible to distribute previously compromised keys to POIs with previously authenticated commands
Normative Annex B

Key-Injection Facility Security Requirements

Same Control Objectives and the applicable requirements as the main body of the PIN Security Requirements

Provides specific criteria pertaining to entities that operate key-injection facilities for the injection of keys used for the acquisition of PIN data

Integrated with applicable requirement criteria from the main body

Normative Annex A may also apply

- Operations of Certification and Registration Authority platforms used in connection with remote key-distribution implementations
- Engaged in remote distribution of symmetric keys using asymmetric techniques
Agenda

Introduction

The Foundation to Build Upon

POI Security Requirements v3.1

PIN Security Requirements v1.0

What’s Next

Open Mic
What’s Next

HSM v2

Update attack methodologies more consistent with POI v3

Update algorithms
  • Minimums
  • Reference standards

Remote key loading criteria
PTS Resources

Payment Card Industry (PCI)
PIN Transaction Security (PTS)

Device Testing and Approval Program Guide
Version 1.1
October 2011

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

Modular Derived Test Requirements
Version 3.1
October 2011

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

Modular Evaluation Vendor Questionnaire
Version 3.1
October 2011
Summary

**Vendors** with clients looking to gain advantages under the P2PE initiative should update their product lines to reflect the new approval classes as well as incorporate SRED into their v2 and v3 POI products.

**Merchants and other entities** wishing to enhance account data protection should use the PTS listings and work with their vendors and processors/acquirers to implement devices with approved SRED functionality.

**All entities** involved in the acquisition of PIN based transactions should familiarize themselves with the PCI PSR and make necessary changes.
Questions?

Open Mic

Please visit our website at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)