Security Standards Council

Understanding the PTS Security Requirements Version 3.0

Jeremy King
PCI SSC PTS Working Group
May 2010

AGENDA

PTS Security Requirements 3.0

Modular Approach

New Modules and Updates

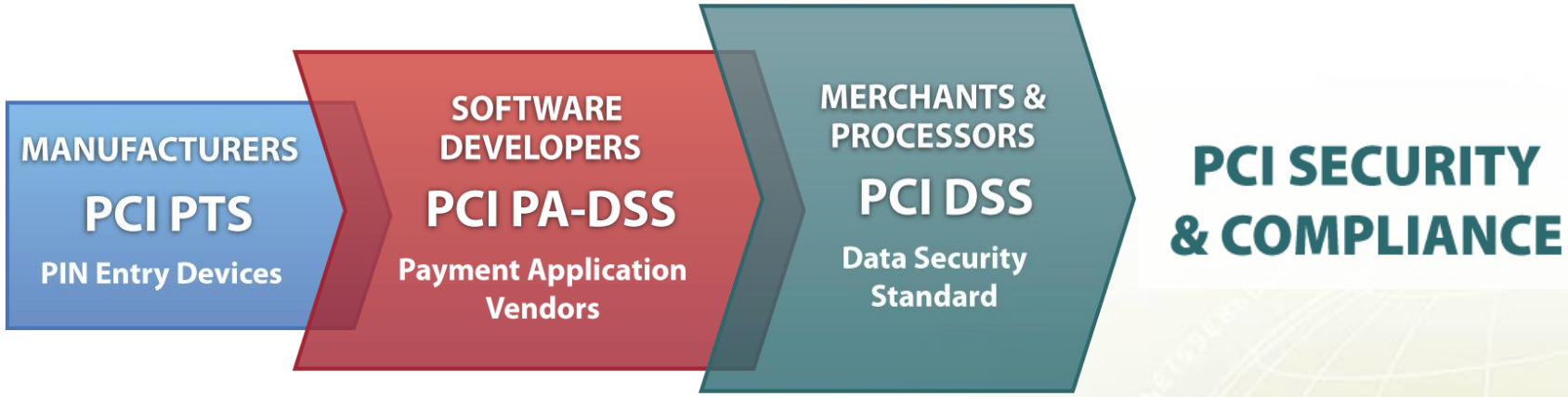
PCI SSC Resources

Security Standards Council

PTS Security Requirements 3.0

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

PTS Program Overview

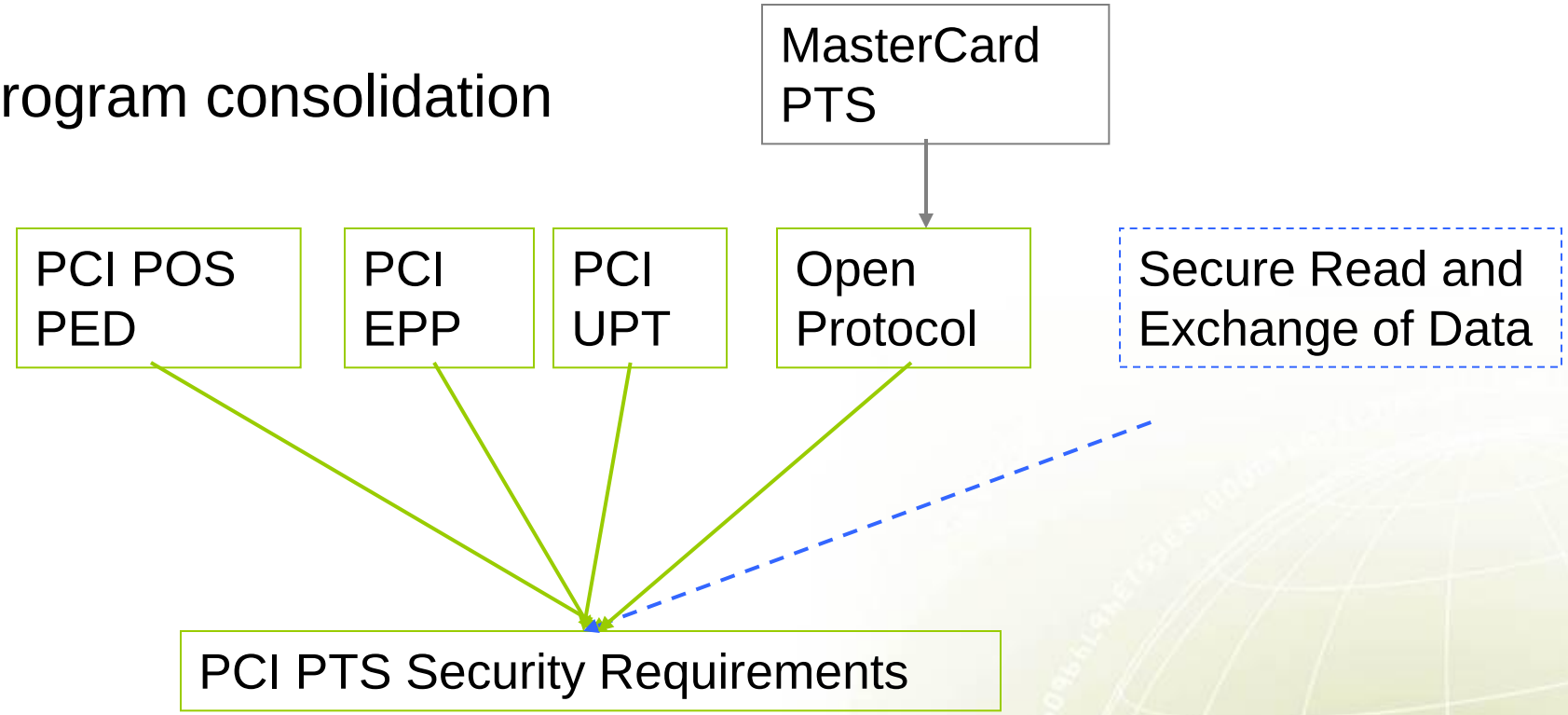
- Version 3.0 represents a significant change to the layout, format and scope of what was the PCI POS PED Security Program:
  - Widening the scope of the evaluation to include:
    - POS PED devices
    - Encrypting PIN Pads
    - Unattended payment Terminals
  - Introduction of Modular Approach
  - New Modules added
    - Open Protocols
    - Integration
    - Secure Read and Exchange of Data (SRED)

PCI PTS Development Lifecycle

- The PCI PTS working group works to a three year lifecycle
  - First year: Discuss and develop new requirements
  - Second year: Update, review & release PTS POI documents
  - Third year: Implement new requirements for all new terminals
- The PCI PTS working group actively support suggestions, reviews and comments on improving security standards
- PCI PTS Working group release the new document to all Participating Organizations for comment and review ahead of formal release
- Once completed the new version is released one year in advance of effective date to allow vendors the opportunity to design new terminals against the new requirements

PCI PTS Security Requirements 3.0

Program consolidation



Security Standards Council

Modular Approach

What is the Modular Approach?

- In order to streamline documentation and integrate all options into a single set of requirements, PCI SSC has moved to a modular approach
- Requirements are now grouped into the following modules
  - Integration (where individual components are brought together into a single product)
  - Core PIN Security Physical
  - Core PIN security Logical
  - Open Protocols (remote logical attacks, addressing Open protocols Software)
  - Secure Read and Exchange of Data (method of securing the cardholder data when entered into the POI)
  - Device management

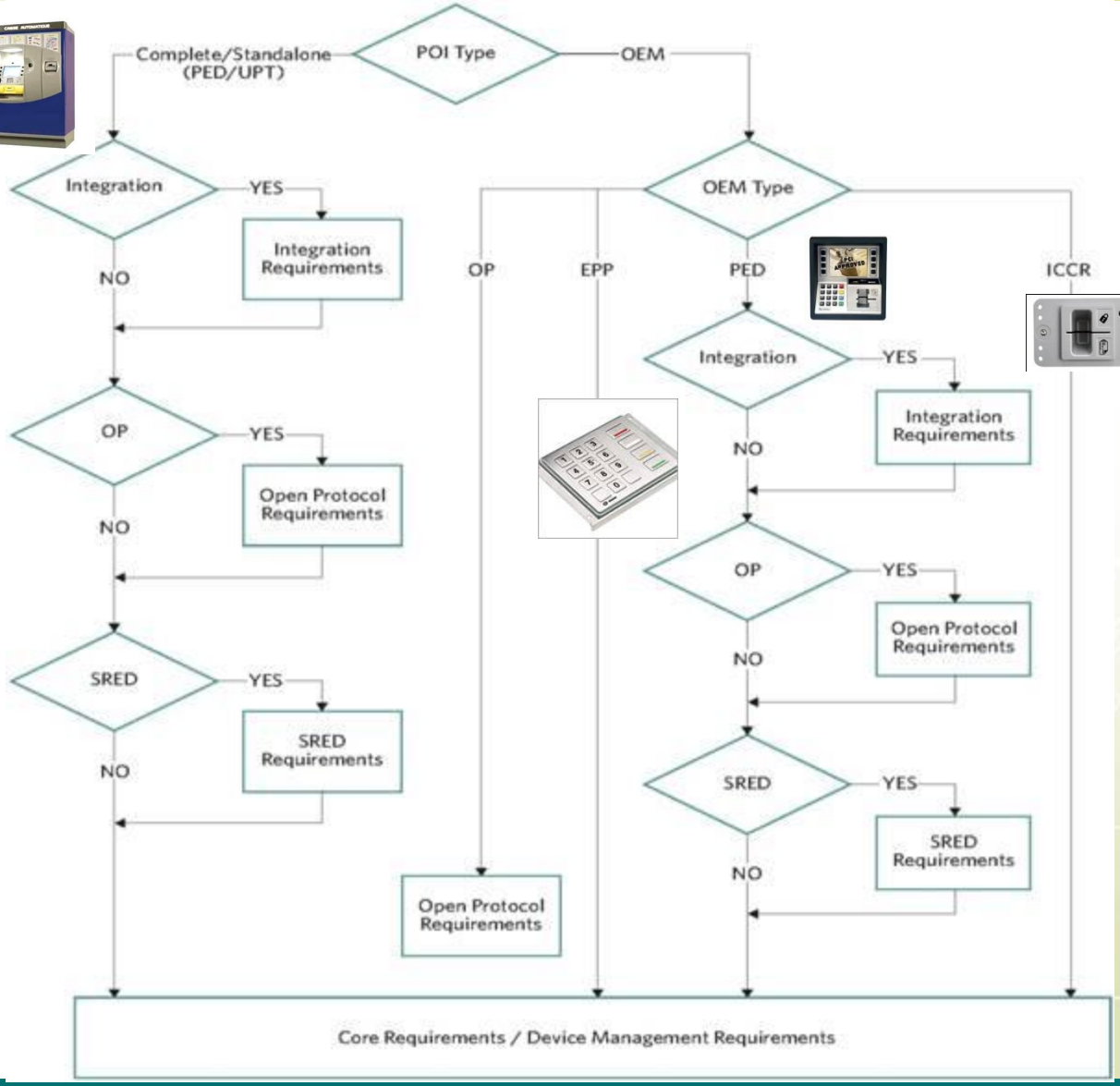
Categories of PCI PTS Products

POI PIN Entry Terminal

OEM Components: EPP,PED,SCR

Integrated POI PIN entry Terminals

Applying the products to the flow chart



Devices not included in the PCI PTS space

- ECR with mag stripe reader
- HSM
- ATM
- Mobile phone with mag stripe reader

PCI HSM

Scheme Specific

Improved Web Listing

Product listing as it will appear on the PCI SSC web site

Verifone

Commercial Name	Photo	Approval Number	Requirements version	Product Type	Expiry date	Approved Components
Vx610		4-30015	PED V1.x	PED	30 Apr 2014	SRED[1] Open Protocol[1]

hardware # : M256-xxx-3x-xxx
firmware # : QB0111A0,
QB0111A1,
QB0111A2
applic # :

Vendor details for PED

Product listed as a PED

Platform Identifier

Vx510, Vx570, Vx610, Vx670, and Vx810

Hardware # : M251-xxx-xx-xxx
M257-xxx-xx-xxx
M256-xxx-xx-xxx
M281-xxx-xx-xxx

Firmware # : Verix V Operating System

Applic. # : TCPIP 3.x.x and UCL 2.x.x

Vendor details for Open Protocols

Note 1: Example of how SRED and OP modules will be represented on the web site listing

Security Standards Council

New Modules and Updates

What are they?

- Open Protocols
  - Ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities
  - Covers IP connectivity (internet), GPRS, Wifi
  - Integration
  - Ensures integration of previously approved components does not impair the overall security as stated in security requirements
  - Supports the cost-effective maintenance of components
- Secure Read and Exchange of Data (SRED)
  - 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.
  - Secure first step for Point to Point or end to end encryption

Open Protocols Module

- Open Protocols
  - A set of requirements that ensures PIN entry devices using open security protocols and open communication protocols to access public networks and services do not have public domain vulnerabilities
  - Covers IP connectivity (internet), GPRS, Wifi

Why are Internet and Wireless POS terminals so popular?

- Convenient
  - Fast
  - Seamless integration into merchant networks
  - Embedded security and device management
  - Cash replacement niches (mobility, vending machines)
- Low cost
  - Payment devices
  - Communication
  - Deployment
  - Short application development
- High growth area
  - Available for all terminal types
  - Increasingly popular i.e. pay at table
  - Permits use in non fixed locations

Stand alone POS terminals

- POS terminals commonly used in stand alone mode
- Open Security Protocols **(IP stack and wireless stacks of protocols)**
- Usually in small merchants
- Exposed to hackers

POS terminal and PINpad

Integrated POS terminal/PINpad

Allows criminals to use same attack techniques used against PC's on the internet

Risk of data compromise; remote exploitation of vulnerabilities in Open Protocols

Open Protocols

The PTS Open Protocol Module will Check the IP protocols (e.g. SSL, TLS, ICMP, TCP) and services (e.g. DHCP, HTTP, FTP) that are used, by:

- Reviewing documentation
- Testing the implementation
  - Port scanning: inventory of resources (ports, protocols, services, OS, …)
  - Vulnerability scan
    - Identify vulnerabilities and wrong configuration
    - Ensuring compliance with security policies
  - Penetration scan
- Validate the mechanisms implemented to assure confidentiality, integrity, authentication

Integration Module

- This is a new module which covers those situations where OEM components are brought together to form a single product
- The requirements are designed to ensure that when the components are brought together they do not introduce any security weaknesses

Definition of Integration

Integrated device; EPP, card reader and display are integrated into an OEM PED

Integrated device; the EPP, card reader and display are integrated into the UPT

Integrated device; OEM PED is integrated into a fuel pump

Above are NOT integrated devices

Secure Read and Exchange of Data (SRED)

What SRED is….

- The first stage that introduces a secure evaluation process within the PIN Transaction Security Evaluation Program

- It establishes the requirements we would expect to be satisfied if a PIN Entry - Point of Interaction device is used to encrypt transaction and cardholder data

What SRED is Not…

- A solution for End to End Encryption

- A comprehensive statement on how to do transaction data encryption that will meet all DSS requirements

- The only path to implementing secure transaction data encryption

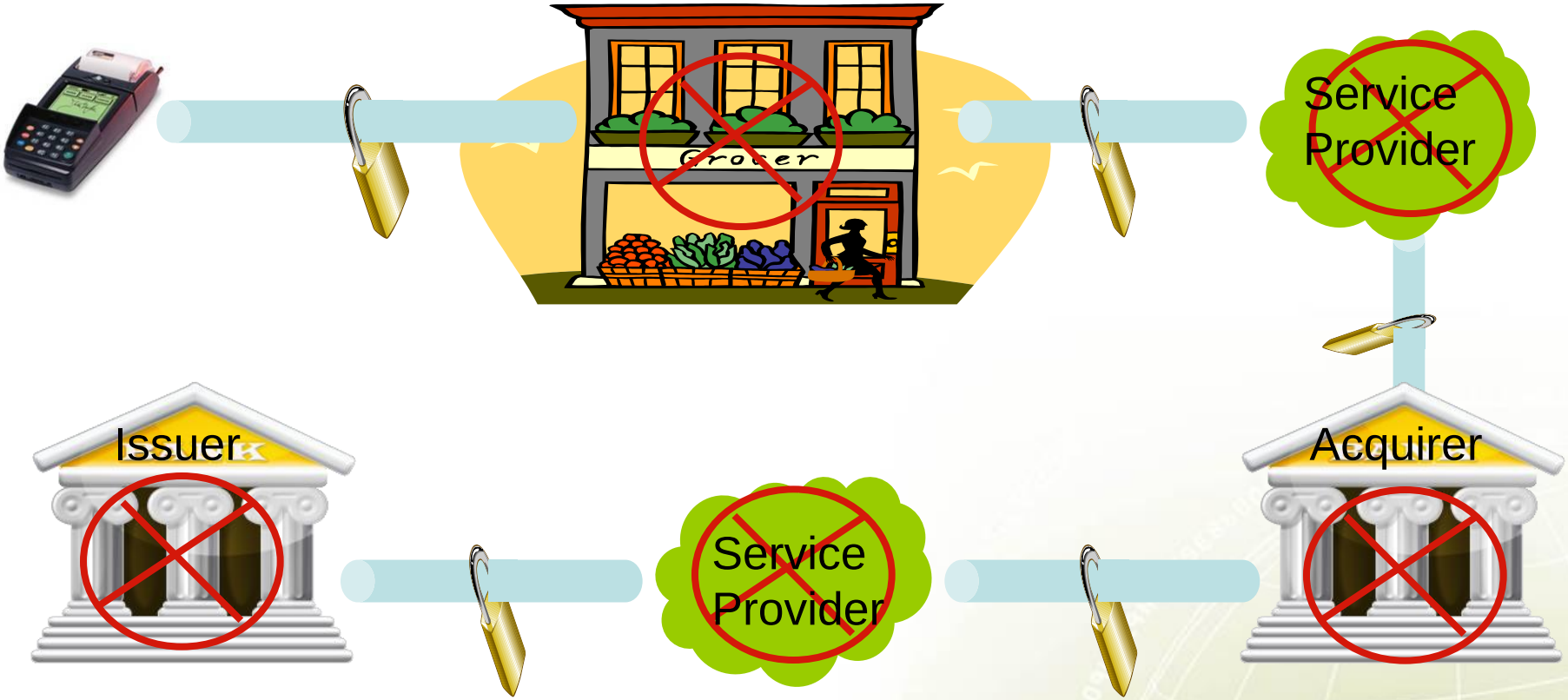
SRED Explained

- PIN Enabled devices
  - Enabling infrastructure at PTS
    - Secure HW resources already in the device
    - Evaluation at the PTS framework readily available
    - Utilizing evaluation laboratory skills to evaluate solution
  - Supports and plugs into DSS requirement 3.6
  - Architectures supported
    - Encrypting mag. stripe read head
    - Standard mag. Stripe read head
    - Chip reader
    - Key management structure

The Process - the simple view

- Common misconception: (1) the data is entered securely and encrypted in the PED, and is then sent to the bank where it is securely decrypted, verified and approved, and (2)therefore the merchant has no involvement in the process and thus meets the requirements of PCI-DSS

The Process – how does it work?



- Depending on the architecture data could be decrypted and re-encrypted at every stage of the process, introducing significant new approval and management challenges

SRED - Terminal Manufacturers

- Introducing a Secure Reading and Data Encryption module into PTS provides a secure method for data encryption within the terminal
- Depending upon the solution part of the PAN may remain in clear text for routing or chargeback issues
- SRED enables the terminal to be authenticated to the merchant location

- **NOTE: This only applies to PIN Entry Point of Interaction devices**

In Scope

Out of Scope

SRED - Merchants

- If they wish, merchants can simply pass the data through – easiest solution
- However if they wish to manage the data themselves, merchants should ensure:
  - The data is unencrypted and re-encrypted in a secure manner, such as by using a council approved HSM
  - Use of appropriate strong Key management procedures with clearly defined roles
  - The Key management procedures are assessed by the council
- The merchant must continue to meet all PCI-DSS requirements

PCI Approved HSM

SRED - Service Providers

- Requirements are very similar to the merchant
- If they wish they can simply route the information through as is
- If the data is unencrypted and re-encrypted, then this must be undertaken in a secure manner, such as by using a Council approved HSM
- Using appropriate strong Key management procedures with clearly defined roles
- Again The PCI Council will need to assess the Key management procedures

This is only the Start – the first step

- The point of entry for cardholder/account data is a critical first base to secure, but is just one part of the process
- For Secure Reading and Exchange of Data (SRED) to take place, it is essential that the initial data entry is undertaken in a controlled, evaluated and secure manner
- The SRED module in the PTS process enables this to be evaluated and approved
- This process does not go beyond the PIN Entry POI Device and is only one component of an approach to point to point encryption

Additional Updates

- Changes to Points System
  - Version 3 introduces a minimum standard for Exploitation with the aim of making it difficult for the criminals every time to succeed
  - The overall points required for some aspects has increased
- Enclosure –Integration Requirements
  - To address recess abuses
  - Take into account specificities of large cabinets (UPT)
- For compound devices, make sure that:
  - All components integrate well together
  - OEM sec mechanisms are well implemented

Security Standards Council

PCI SSC Resources

Need More Information?

Council Resources

- Security standards and supporting documents

- Quick Reference Guide

- Searchable Frequently Asked Questions

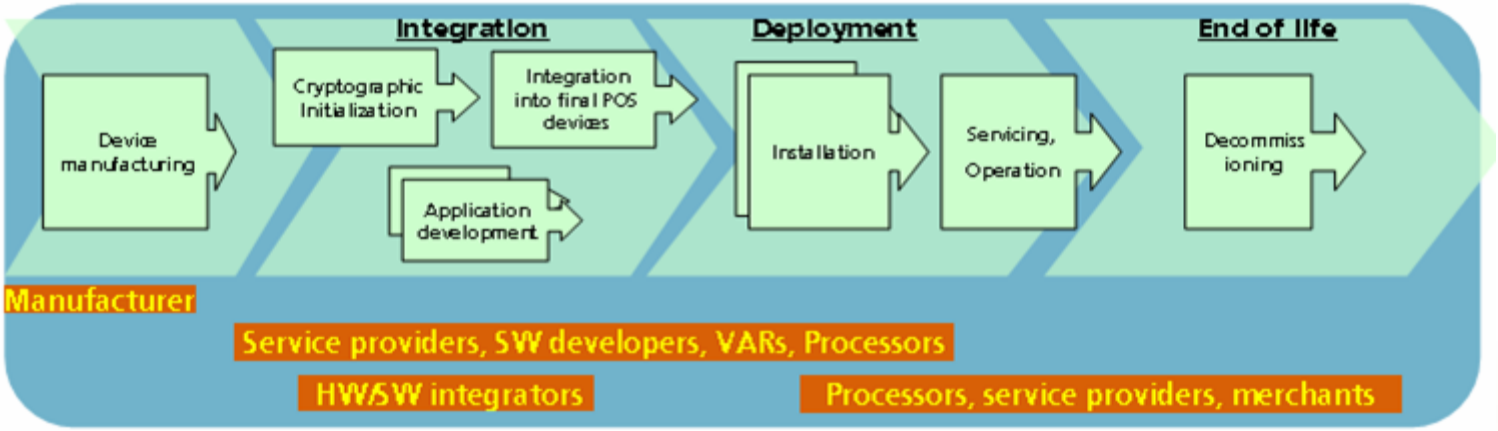
- List of approved PED Labs, QSAs, ASVs, PA-QSAs,

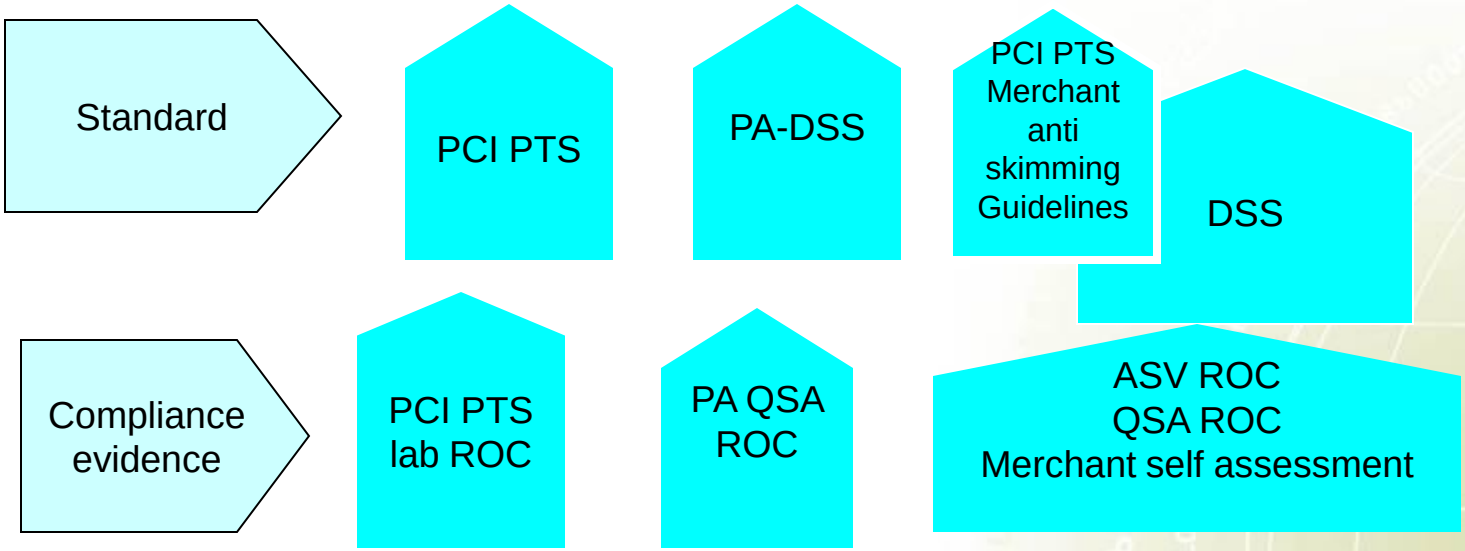
- Education and outreach - e.g., fact sheets, webinars

- Participating membership, meetings, collaboration

- A global voice for the industry

PCI PTS, DSS and PA-DSS assessments are complementary





Summary

- PTS Security Requirements v 3.0 make it easier for device vendors and their customers to secure sensitive card data at the point of interaction and are a critical part of any payment security strategy
  - Provides one security evaluation program simplifying and strengthening existing requirements to increase security
  - Expands scope by adding three new modules for open protocols, integration and secure reading and exchange of data
  - Gives vendors clear criteria to test and building against
  - Ensures a device helps, not hinders in a merchant's PCI DSS compliance efforts
  - Offers new and improved device listings and supporting resources at the Council website: https://www.pcisecuritystandards.org/security_standards/ped/index.shtml

Security
Standards Council

Thank You