



MasterCard
Worldwide

Security & the Payment Systems

POS PED, PTS, and PA DSS

Agenda

- Point-of-Sale PIN Entry Device
- Point of Sale Terminal Security Program
- Payment Application Data Security Standard

Jeremy King
Vice President, Payment System Integrity



Point-of-Sale PIN Entry Device

POS PED

What is a PED?



Secure method for performing a credit or debit transaction at a merchant location

PIN Entry Device consists of a PIN Pad, Display and generally a Card Reader

Allows for secure entry and processing of the cardholders PIN



Encrypting PIN Pad (EPP)



Secure unit for entering
and encrypting
cardholder PIN usually
used at ATM and other
unattended Terminal

No display or card reader



PED Security Overview

- PED is a fundamental component to:
 - fulfill product security requirements
 - authenticate cardholders
 - provide security services to POI terminal
 - provide assurance to cardholder
- Most PEDs are deployed in hostile environments

Why raise Security Levels

- PEDs are becoming progressively more complex
- PEDs are multi-functional devices that:
 - support magnetic stripe and chip transactions
 - accommodate multiple applications (payment and non payment)
- PEDs can fall into the hands of attackers
 - in unattended locations
 - when unconnected (wireless) PED

Short History Of PED

- Pre-2002
 - Terminals which were never approved in an evaluation laboratory
 - Minimal security
 - Mostly removed by switch to Chip and PIN in UK
- 2002 – 2004 Visa PED Approved
 - Form the majority of PEDs in use in the UK
 - Good level of security at the time
 - Problem now is that increasing number are being compromised
 - Approvals lapse 31st December 2007
- 2005 Onwards PCI POS PED
 - High Level of Security

What is PCI Doing to Improve Security?




- PCI has standardized a set of security requirements for all POS PED terminals
- These requirements specifically address the physical and logical security of the POS PED
- The requirements will:
 - Ensure it is very difficult time consuming and costly to insert a skimming bug
 - Ensure it is extremely difficult and costly to obtain secret information from the POS PED device
- These requirements are global

More Information can be found on MOL

- Security & Risk Svcs
- PIN, Terminal and WLAN
- PEDs & Epps

Contact:
PED@MasterCard.com



Vendor Publications - Microsoft Internet Explorer provided by MasterCard International

Address: https://inbe20101.mastercard.net/inbe20102/one-vent/library/vendor_jsp/MainMenu.html

MasterCard International **Vendor Publications** MasterCard OnLine

Libraries

- Europe
- Spain
- Portugal

Manuals

- List of Manuals
- Recently Published
- Manuals by Category
 - Authorization
 - Clearing
 - Debit
 - Electronic Commerce
 - File Transfer
 - MasterCom Systems
 - Prepaid Solutions
 - Reference
 - Security/Risk Svcs**
 - Settlement
 - Smart Card

Recently Published

- Internet IP-Enabled POS Terminals—SSL/TLS Implementation Guidelines
- Internet IP-Enabled POS Terminals—Security Guidelines
- MasterCard Dictionary
- MasterCard PCI—PED and EPP Approval List
- MDS Settlement and Reports

News

Reorganization of Smart Card Documents
MasterCard has reorganized the Smart Card manuals into new subcategories to make it easier for you to find needed information. This new cascading menu structure is available when you click on the Smart Card button in the "Manuals by Category" area of any of the global menus

Tip of the Month

PCI PED Security Evaluation Program—Program Manual

PCI POS PIN Entry Device Derived Test Requirements

PCI POS PIN Entry Device Evaluation Vendor Questionnaire

PCI POS PIN Entry Device Security Requirements

Leader

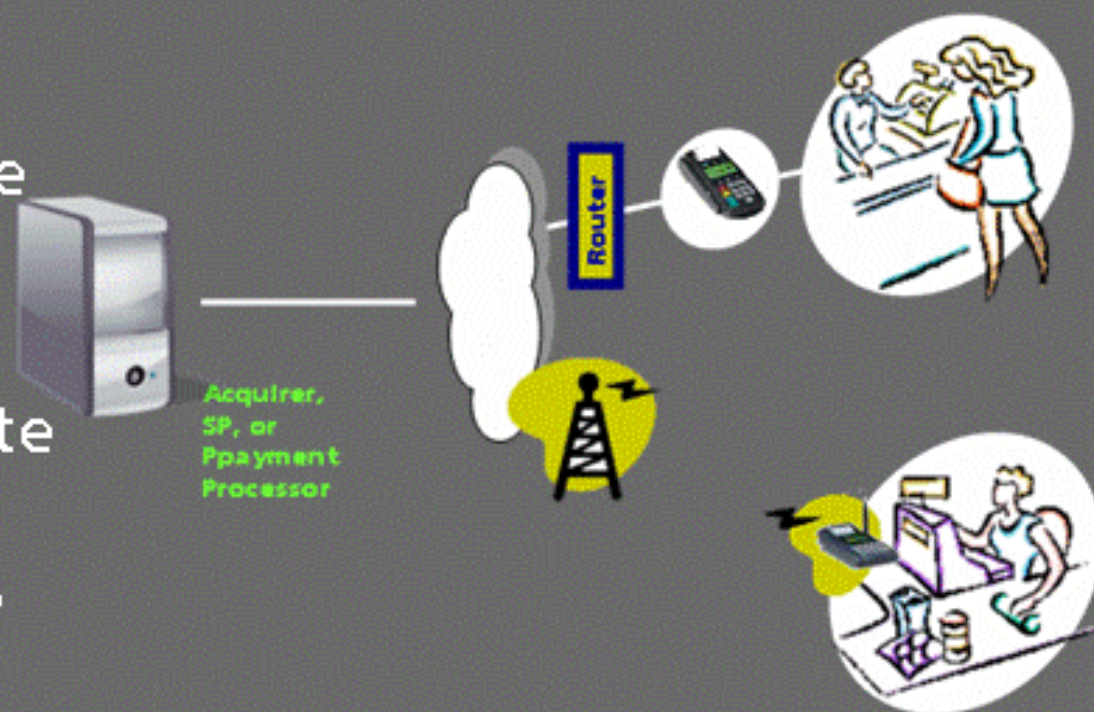
Point of Sale Terminal Security Program

PTS

PTS (Point of Sale Terminal Security) Program: What is it?

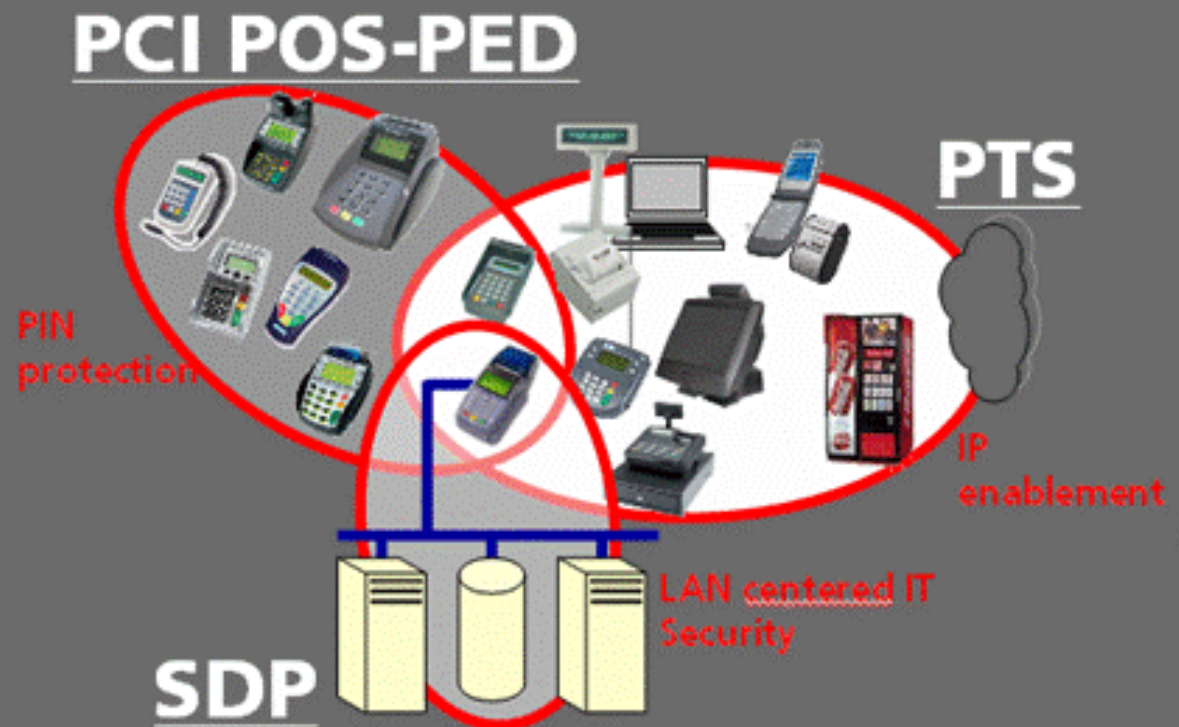


- Security validation program for POS terminals (POS terminal security is assessed by independent laboratory)
- Applicable to stand-alone POS terminals (that are exposed to the Internet or wireless networks)
- Main focus: secure implementation of the internet protocol set
- Protects against remote theft of sensitive information from POS terminals



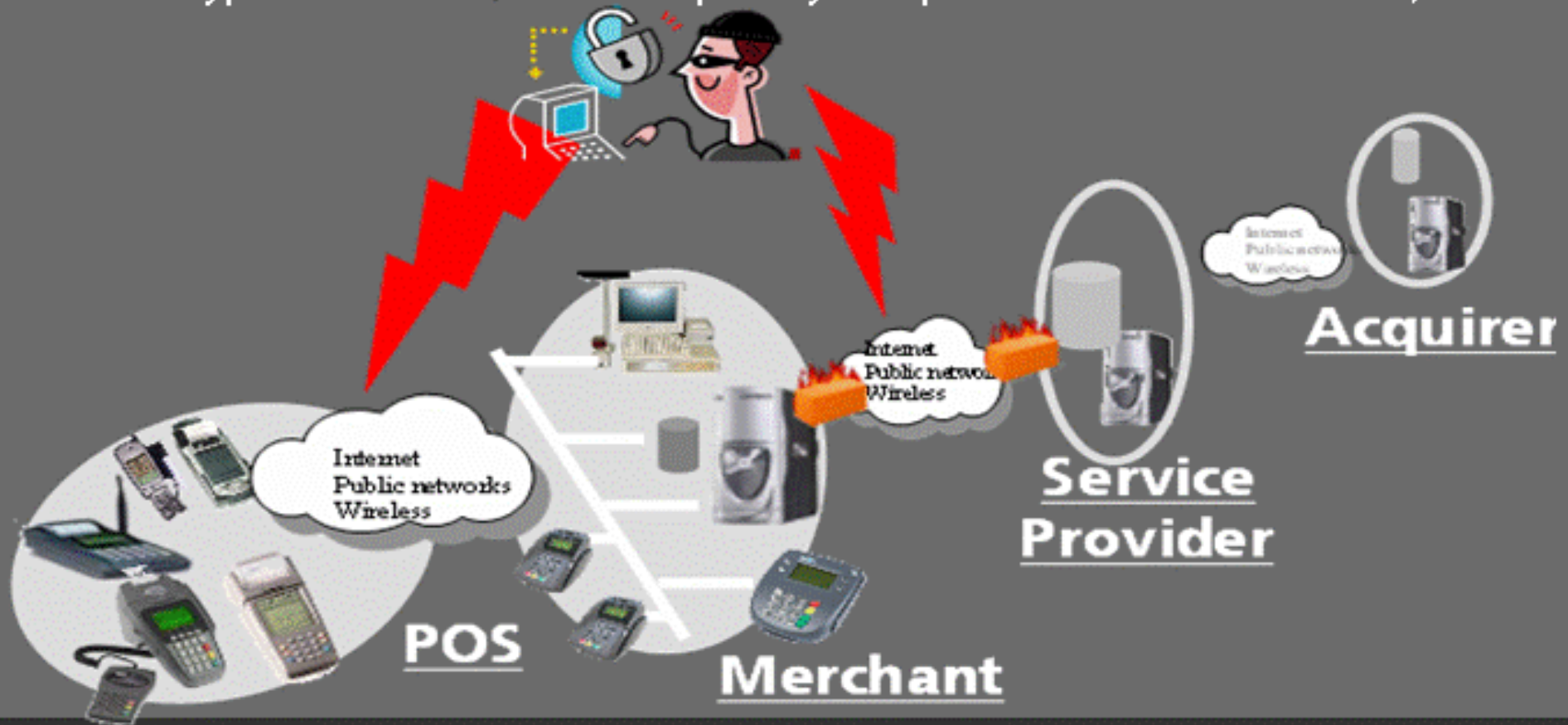
PTS Program: Where does it fit?

- One component of the MasterCard security initiatives for the Point of Sale:
 - POS encryption mandate
(wireless and IP enabled POS terminals)
 - PCI POS-PED program
(PIN entry devices for POS terminals)
 - SDP program
(based on PCI DSS)



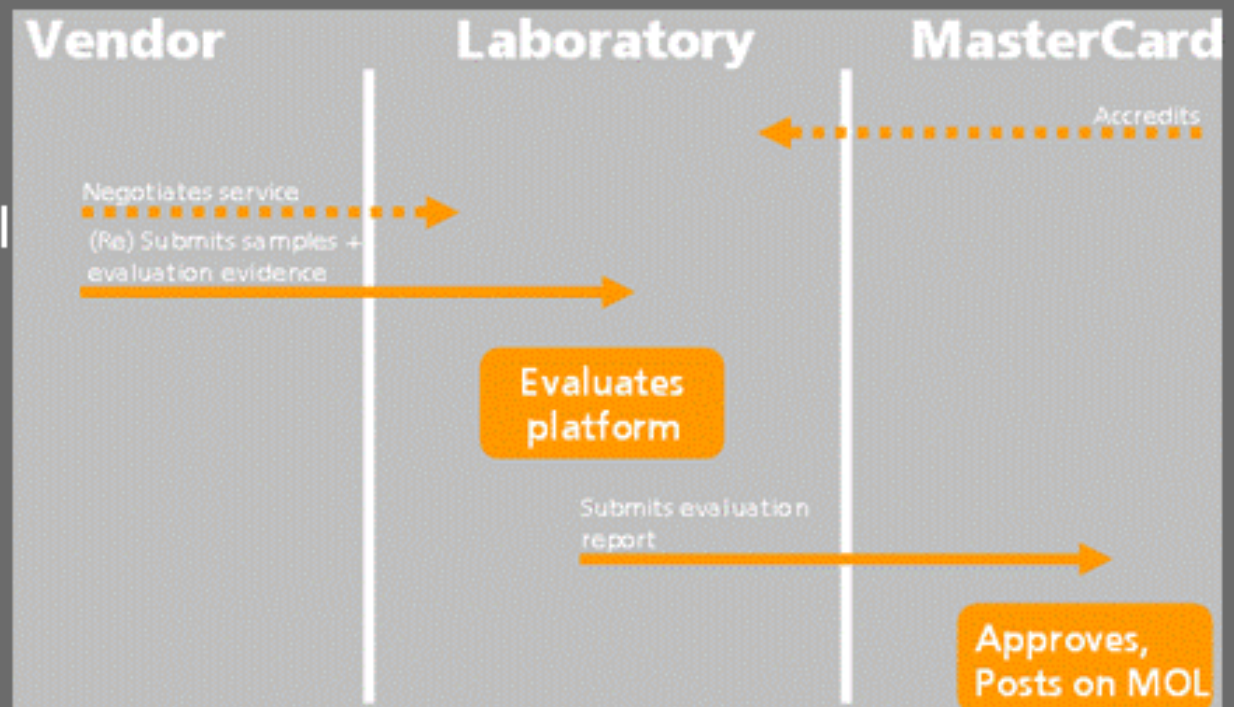
What/where are the benefits of PTS?

- Ensures that POS terminals have a minimal level of security against remote attackers
(the same type of attackers who frequently compromise merchants' LANs)



Constituents and roles

- MasterCard acquirers (or their agents)
 - Must ensure that PTS approved POS terminals are used at their merchants
- Terminal vendors
 - Should submit terminal for validation at PTS accredited laboratories
- MasterCard
 - Upon successful validation by laboratory, updates PTS approval list



How to get started/comply with PTS



- MasterCard acquirers (or agents) must seek compliant terminals in the PTS approval list
- Terminal vendors selling POS terminals to MasterCard acquirers, POS terminal integrators, application developers, transaction processors, etc, should request:
 - PTS Program Manual
 - PTS Security Requirements
 - PTS Questionnaire



POS Terminal Security Program

Approval List

Approved Platforms

Apeiva.....	1-1
Axalto S.A.....	1-1
Hypercom.....	1-2
Ingenico.....	1-2
SAGEM Monetel.....	1-3
Verifone Inc.....	1-3
XAC Automation Company.....	1-4



Contact: PTS@mastercard.com



Members and vendors

mastercardonline.com

(publications section)

MasterCard OnLine
Member Publications

Libraries
Europe
Español
Português
Smart Data

Manuals
List of Manuals
Recently Published

Manuals by Category
Authorization
Card Design
Clearing
Commercial Products
Debit
Electronic Commerce
File Transfer
MasterCom Systems
MIBS
Prepaid Solutions
Reference
Risk Management
RPPS
Rules
Security/Risk Tools

MasterCard OnLine - Publications
All
ENS Alerts Quick Reference Guide
Fraud Monitor Alerts Quick Reference Guide
Fraud Reporter Users' Manual
Issuers' Clearinghouse Service Operations Manual
Issuers' Clearinghouse Service Quick Reference Guide
Logical Security Requirements for Card Personalization Bureau
MasterCard Physical Security Standards for Plastic Card Vendors
MasterCard Registration Program Users' Manual
MATCH Users' Manual
Message Integrity Guidelines
HOST Users' Manual
PIN, Terminal, and Wireless LAN
Risk Finder Alerts Quick Reference Guide
SAFE
Security Rules and Procedures
Security Standards for Instant

Search

Support
Help
Site In
New Us
E-mail
Contact
POS Terminal Security Program-Approval List
POS Terminal Security Program-Derived Test Requirements
POS Terminal Security Program-Program Manual
POS Terminal Security Program-Security Guidelines
POS Terminal Security Program-Security Requirements
POS Terminal Security Program-SSL/TLS Implementation Guidelines
POS Terminal Security Program-Vendor Questionnaire

the Month to locate recent changes online? You can search on the date. Learn more.

MasterCard Worldwide
United States - English
Contact Us FAQs

Home Personal Cards For Business For Merchants Company Info

Merchant Home Page
Start Accepting MasterCard
Benefits of Accepting MasterCard
How MasterCard Works
Solutions & Resources
Security

What You Can Do
Get It Started
Card Identification
Essentials
PTS Program
Online and Catalogs
MasterCard SecureCode

Point of Sale Terminal Security (PTS) Program & the Encryption Requirement

Your tools for security success

Security Solutions to Prevent Fraud
The MasterCard Point of Sale Terminal Security (PTS) program was announced in September 2005 together with a global encryption requirement for data exchanged by wireless POS terminals and Internet/Stand-alone IP-enabled POS terminals. As of January 2007, all acquirers have to replace noncompliant wireless POS terminals and Internet/Stand-alone IP-enabled POS devices with terminals that meet the data encryption requirement and all PTS security standards.

Objectives and Scope
The objective of the security evaluation program for Internet Protocol-enabled POS devices is to ensure the necessary level of protection for transaction and cardholder data at Merchants that use equipment that support the TCP/IP protocol suite. The security evaluation verifies that POS devices meet the relevant MasterCard requirements in terms of confidentiality, integrity and authentication, and authorization. By addressing the objective of POS terminals to

Merchants

mastercardmerchant.com

(security section)

Payment Application Data Security Standard

PA DSS

What is PA DSS?

- Payment Application Data Security Standard (PA DSS)
- MasterCard is working as Part of PCI SSC to incorporate a Payment Application Standard that is separate from the PCI DSS.
- PA DSS is a Payment Card Industry program created to assist vendors in developing and delivering secure payment applications to the market.
- High Level Goals:
 - Provide a framework for secure payment applications which protect merchants and service providers from loss of sensitive data
 - Provide merchants and service providers with a listing of payment application approved vendors

Why is PA DSS good for the Payment Industry?



- PA DSS is aligned with PCI DSS and shares the common goal of reducing the risk of compromising full magnetic stripe data, which includes cardholder data.
- Provides guidance and consistency in the Payment Application community to ensure ongoing vigilance towards industry related threats

Who's affected by PA DSS?

Who does it apply to?

- Point of Sale Application Vendors
 - Software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold or distributed to third-parties.

Who benefits?

- Acquiring Banks
 - Provides Acquiring Banks with the opportunity to ensure their merchants and service providers are utilizing only approved applications which have been certified via PA DSS requirements
- Merchants and Service Providers
 - Organizations can choose from those payment applications which have been certified to enable their PCI Compliance initiatives

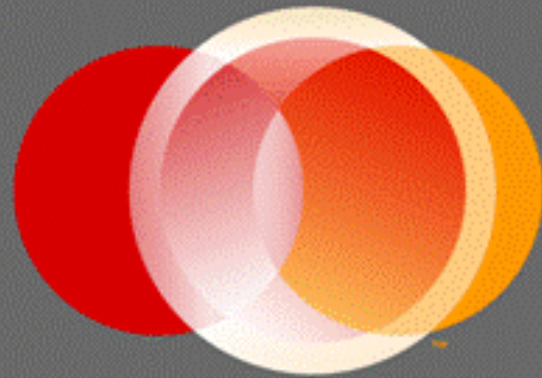
PA DSS Adoption Timeline



Milestone	Deliverable	Target Date
Comment Period	PCI SSC member feedback period and updates to the standard	Oct 2007
Payment Application Data Security Standard and Testing Procedures v1.0	PCI SSC officially releases PA DSS and Testing Procedures	4Q' 2007
PA QSA List	PA QSA List published on PCI SSC website	2Q' 2008
Validated Payment Application List Published	Publication of validated (and transitioned) payment applications on PCI SSC website	3Q' 2008

All information will be posted to the PCI SSC Website <https://www.pcisecuritystandards.org/>

Thank you.



MasterCard
Worldwide

The Heart of Commerce™