



AIS Webinar

PA-DSS Program Overview

Hap Huynh
Business Leader
Visa Inc.

December 2009

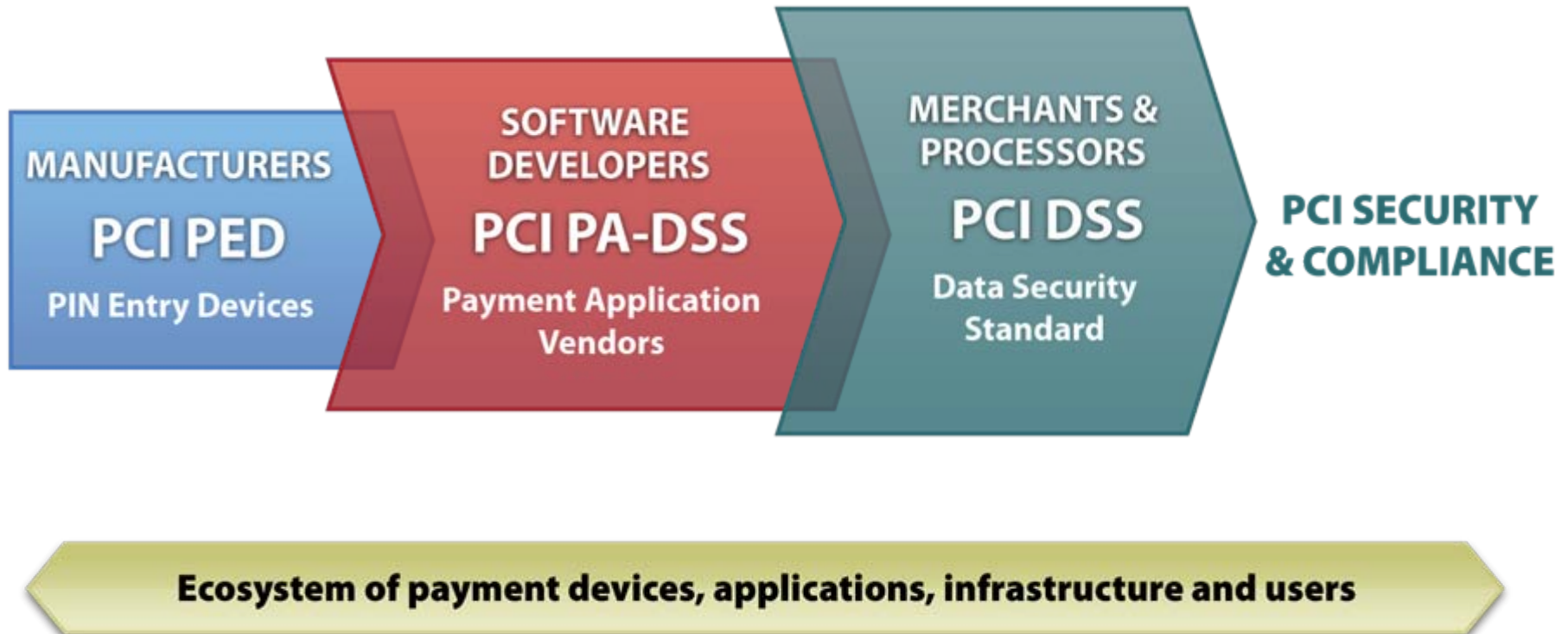
Agenda



- PCI Standards
- PA-DSS Program
- PA-DSS Applicability
- PA-DSS Roles & Responsibilities

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI Standards



- **PCI PTS** (*formerly PCI PED*) covers device tamper detection, cryptographical processes, and other mechanisms used to protect the PIN
 - Encrypted PIN is passed to payment application or hardware terminal
- **PCI PA-DSS** covers secure payment applications to support PCI DSS compliance
 - Payment application receives card data from PEDs or other devices and begins payment transaction
- **PCI DSS** covers security of the systems and networks that store, process, or transmit card data
 - Systems and networks receive card data from payment application and other sources (e.g., acquirers)

Payment Application Security



Visa leads the industry in promoting secure payment applications in the marketplace



Payment Application Data Security Standard



PCI SSC adopted PABP as the PA-DSS in April 2008

- **PCI SSC is responsible for:**
 - Maintaining and updating the PA-DSS and related documentation
 - Qualifying and training Payment Application Qualified Security Assessors (PA-QSAs) to perform PA-DSS assessments
 - Being a single point of repository for PA-DSS Reports of Validation (ROVs)
 - Performing quality assurance reviews of PA-DSS ROVs to confirm report consistency and quality
 - Listing PA-DSS validated payment applications on the PCI SSC website
- **Visa will continue to:**
 - Work with PCI SSC for potential enhancements to address emerging risks
 - Maintain a list of vulnerable payment applications that are known to store prohibited data
 - Promote payment applications that support PCI DSS compliance

Visa Inc. Global Payment Application Framework



»» Newly established global payment application security framework to promote use of secure applications

Payment Application Security framework includes:

- **Global list of payment applications validated against the PA-DSS to be maintained by PCI SSC**
- **Global Visa mandates for use of PA-DSS compliant applications**
 - July 2010, acquirers must ensure any newly boarded merchants utilize PA-DSS compliant payment applications or be PCI DSS compliant
 - July 2012, acquirers must ensure their merchants (new and existing) utilize PA-DSS compliant payment applications
 - Global mandates do not supersede earlier regional mandates
- **Global outreach program for clients and payment application vendors to raise awareness of mandates and increase availability of applications for key industries in all regions**

Payment Application Data Security Standard



Payment applications that support PCI DSS compliance

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
2. Protect stored cardholder data
3. Provide secure authentication features
4. Log payment application activity
5. Develop secure payment applications
6. Protect wireless transmissions
7. Test payment applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software updates
11. Facilitate secure remote access to payment application
12. Encrypt sensitive traffic over public networks
13. Encrypt all non-console administrative access
14. Maintain instructional documentation and training programs for customers, resellers, and integrators

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, distributed, or licensed to third parties.

Page 6, PA-DSS version 1.2

Who Does PA-DSS Apply To?



- PA-DSS is applicable to any third-party payment application that stores, processes, or transmits cardholder data as part of authorization or settlement
- Directly affects:
 - Payment Application Providers (software vendors)
- Indirectly affects:
 - Merchants who buy payment applications
 - Service providers who buy payment applications



PA-DSS Applicability



- PA-DSS **does** apply to payment applications that are typically sold and installed “off the shelf” without much customization by software vendors
- PA-DSS **does** apply to payment applications provided in modules, which typically includes a “baseline” module and other modules specific to customer types or functions, or customized per customer request
 - PA-DSS may only apply to the baseline module if that module is the only one performing payment functions (once confirmed by a PA-QSA)
 - If other modules also perform payment functions, PA-DSS applies to those modules as well

PA-DSS Applicability



- PA-DSS **does not** apply to a payment application developed for and sold to only one customer since this application will be covered as part of the customer's normal PCI DSS compliance review
- PA-DSS **does not** apply to payment applications developed by merchants and service providers if used only in-house (not sold to a third party), since this in-house developed payment application would be covered as part of the merchant's or service provider's normal PCI DSS compliance

PA-DSS Applicability



- The following list illustrates applications that are **NOT** payment applications for purposes of PA-DSS (and therefore do not need to undergo PA-DSS reviews):
 - Operating systems onto which a payment application is installed (for example, Windows, Unix)
 - Database systems that store cardholder data (for example, Oracle)
 - Back-office systems that store cardholder data (for example, for reporting or customer service purposes)



PA-DSS Applicability – Hardware Terminals



- For hardware terminals, PA-DSS may not apply if all of these items are true:
 - The terminal has no connections to any of the merchant's systems or networks
 - The terminal connects only to the acquirer or processor
 - The vendor provides secure remote:
 - Updates
 - Troubleshooting
 - Access
 - Maintenance
 - Sensitive authentication data is never stored after authorization



PA-DSS Applicability Summary



Type of Payment Application *	Does PA-DSS Apply?
“Off-the-shelf” standard payment applications without much customization	YES
Software developed in modules	YES , applies to any module with payment functions
For hardware terminals	YES , unless terminal meets 4 specific criteria (previous slide)
Software for only one, typically large, customer, developed to customer’s specifications	NO , application is covered as part of customer’s PCI DSS review
Software developed by merchant or service provider, and used only in-house	NO , application is covered as part of merchant’s or service provider’s PCI DSS review
Supporting systems, for example, operating systems, databases, back-office systems, firewalls, routers, etc.	NO , these are NOT payment applications

*Payment applications are those that store, process, or transmit cardholder data as part of authorization or settlement.

Cardholder Data: Important Concepts



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number	YES	YES	YES
	Cardholder Name ¹	YES	YES ¹	NO
	Service Code ¹	YES	YES ¹	NO
	Expiration Date ¹	YES	YES ¹	NO
Sensitive Authentication Data ²	Full Magnetic Stripe Data ³	NO	N/A	N/A
	CAV2/CID/CVC2/CVV2	NO	N/A	N/A
	PIN/PIN Block	NO	N/A	N/A

1. *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*
2. *Do not store sensitive authentication data after authorization (even if encrypted).*
3. *Full track data from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.*

PA-DSS List of Validated Applications



- The PCI SSC has assumed the management of the list of validated payment applications at PCI SSC's website www.pcisecuritystandards.org
- PCI SSC has a process to transfer or “grandfather” payment applications validated against the PABP to the PA-DSS
 - Listed with an expiration indicating a mandatory date for revalidation under PA-DSS
 - PABP validation documents were to be provided to Visa by September 15, 2008 and transitioned to the PCI SSC list
 - If PABP validation was not accepted by November 30, 2008, the application would undergo the PCI SSC's PABP to PA-DSS Transition Procedures in order to be listed
- Visa is committed to working with the PCI SSC to ensure a successful transition of PABP to the PA-DSS

PA-DSS Roles and Responsibilities



- **Software Vendors** - develop payment applications*, and sell, distribute, or license these applications to third parties, and are responsible for:
 - Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance
 - Following PCI DSS requirements if the vendor ever stores, processes or transmits cardholder data
 - Creating a PA-DSS *Implementation Guide*, specific to each application
 - Educating customers, resellers, and integrators on how to install and configure the payment applications
 - Ensuring payment applications meet PA-DSS requirements by successfully undergoing a PA-DSS review

*Payment applications store, process, or transmit cardholder data as part of authorization or settlement

PA-DSS Roles and Responsibilities



- **PA-QSAs** - QSAs that have been qualified and trained by PCI SSC to perform PA-DSS reviews, are responsible for:
 - Performing payment application assessments per the PA-DSS and the PA-QSA Validation Requirements
 - Providing opinions regarding payment applications' compliance with PA-DSS requirements
 - Providing adequate documentation within ROV to show that payment application is PA-DSS compliant
 - Submitting the ROV to PCI SSC, along with the Attestation of Validation
 - Signed by both PA-QSA and vendor
 - Maintaining an internal PA-QSA quality assurance process



PA-DSS Roles and Responsibilities

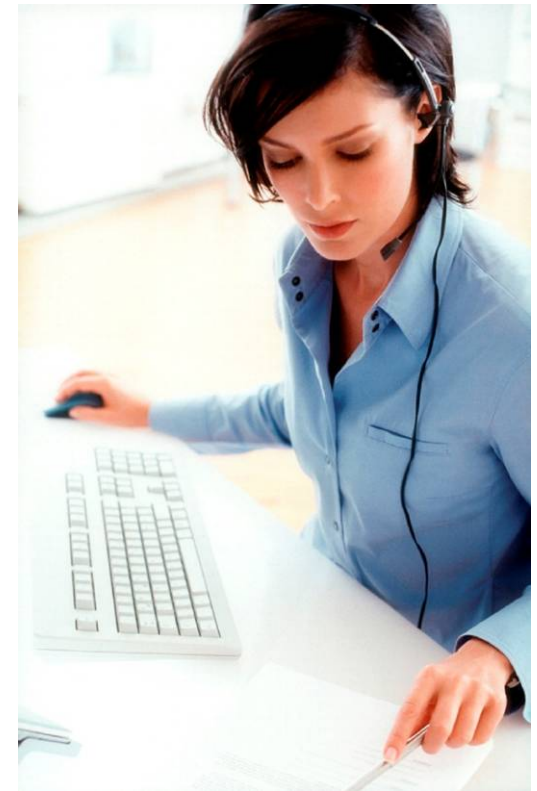


- **Resellers/Integrators** - entities that sell, install, or service PA-DSS compliant payment applications on behalf of software vendors or others, are responsible for:
 - Must implement security requirements as instructed by the vendor's PA-DSS implementation guide and training
 - When installing payment applications, protect customers by following strict security requirements, including but not limited to:
 - Remote management software should be disabled, removed and not used unless necessary and required
 - If necessary, ensure appropriate security controls are implemented to prevent unauthorized access
 - Do not use system default settings and do not re-use the same usernames or passwords for payment applications or any system across multiple customers
 - Advise customers to implement a properly-configured firewall to protect the payment environment from unauthorized access
 - Instruct customers to maintain the latest security patches for the payment application, including the operating system and other necessary software

PA-DSS Roles and Responsibilities



- **Customers** - merchants, service providers, or others who buy or receive a third-party payment application, are responsible for:
 - Implementing a PA-DSS compliant payment application into a PCI DSS compliant environment
 - Configuring the payment application according to the *PA-DSS Implementation Guide*
 - Configuring the application in a PCI DSS compliant manner
 - Maintaining the PCI DSS compliant status for both the environment and the application



Reference Tools



PCI SSC

- PCI Data Security Standard
- PIN Entry Devices Program
- Payment Application Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaires
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

www.pcisecuritystandards.org

Visa AIS

- Archive of Data Security Alerts, bulletins and webinars
- What To Do If Compromised guide
- Qualified Incident Response Assessor List
- List of PCI DSS-Compliant Service Providers
- List of PABP-Validated Payment Applications
- PIN Security Best Practices
- Training

www.visa-asia.com/secured

www.visa-asia.com/padss

vpssais@visa.com

Questions?

