Visa Cemea
Account Information Security (AIS) Programme

Mani Tulasi – Payment Security Risk

November 2008

Content

- Overview Payment Card Industry Data Security Standard (PCI DSS
- Visa's AIS Programme
- Benefits of the AIS Programme
- Compliance Validation Requirements and process

Overview of PCI DSS Standard

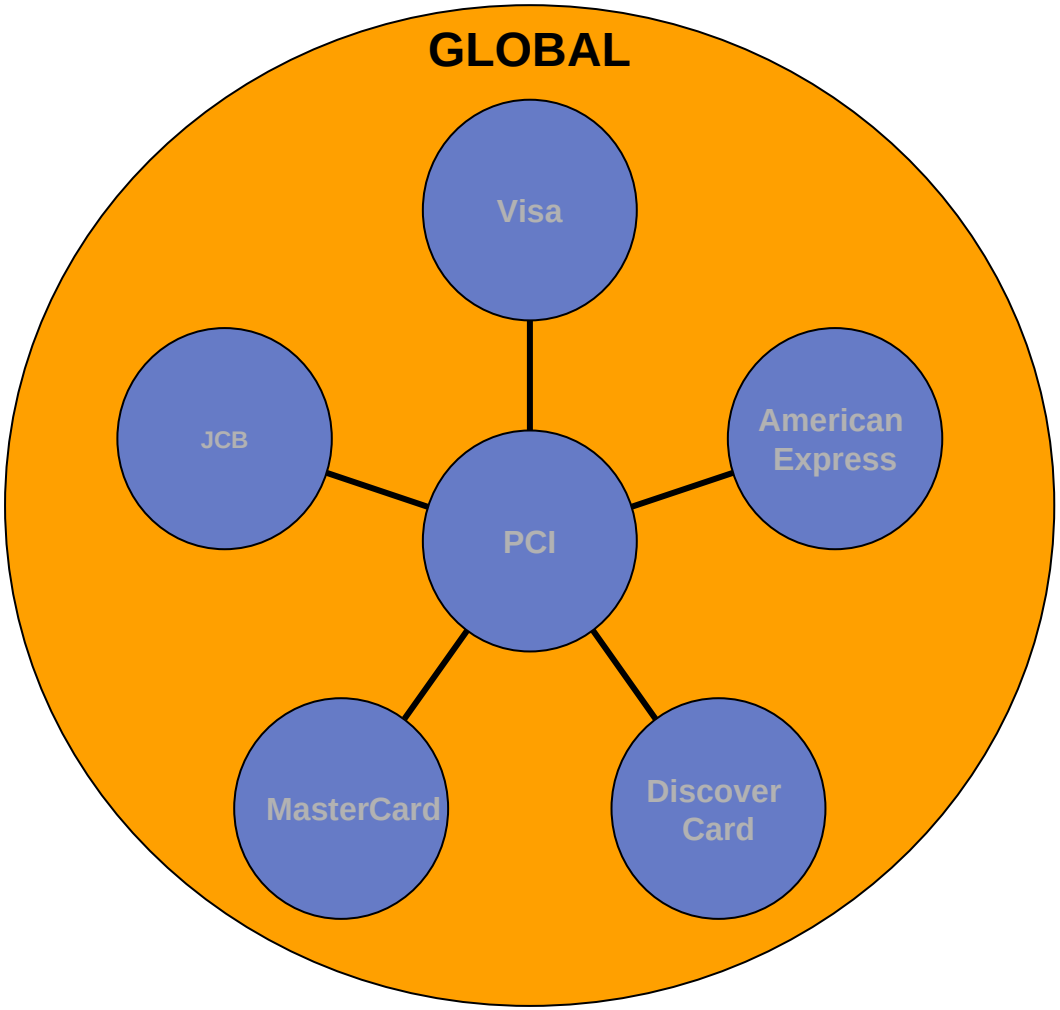
PCI Data Security Standard (PCI DSS)

Original published as the Visa Account Information Security Standard in 2000 and globally mandated in 2001

Growing pressure from the industry to create a single aligned global standard resulted in the alignment of standard with other payment schemes.

Payment Card Industry Data Security Standard published in Jan 2005 as the globally aligned standard supported by the payment schemes participating in the PCI initiative.

PCI Participants



PCI DSS Objectives

The main objective of PCI DSS is to improve the overall level of security for payments globally by:

- Promoting a secure environment for cardholder data
- Reducing inter-scheme redundancies and inconsistencies in requirements.
- Streamlining processes and reducing expenses
- Single validation to satisfy the requirements of all participating schemes.

Elements of PCI DSS Alignment

Aligned Standards and Validation Tools

- PCI Data Security Standard (DSS)
- PCI Security Audit Procedures
- PCI Self-Assessment Questionnaire
- PCI Network Security Scan Requirements

PCI Security Standard Council

To manage the aligned standard, validation tools and centrally manage the process of approving security assessors, the participants of PCI formed Payment Card Industry Security Standard Council (PCI SSC) in Sept 06

PCI SSC is responsible for

- Managing and maintaining the aligned standards including future updates.
- Approving on-site security assessors
- Approving network scan vendors

- PCI SSC is a global forum

Storing Cardholder Data

What is allowed to be stored, transmitted, or processed?

- PAN, and expiration date.

How should the PAN be protected when stored?

- Encrypted, hashed, or truncated

What MUST NOT be stored post-authorization?

- Full track data (Track 1 or 2)
- CVV2
- PIN block/ Clear PIN

Storing Track Data For Troubleshooting Purposes

Sometimes track data must be stored (temporarily) for troubleshooting purposes

Why? Track misreads, network errors, encryption issues, etc.

Procedures should be defined around this issue:

- Retention period
- Destruction procedure
- Limits to number cardholder data stored

Visa's AIS Programme

Visa's AIS Programme

Due to the different business models and legal liabilities, all participants of PCI agreed that each scheme maintain, manage and enforce its own compliance program.

In Visa PCI DSS is validated via the regional Account Information Security Programme.

The programme is known as AIS Programme in all Visa regions, except in US where it is called Cardholder Information Security Programme (CISP)

AIS New Terminology for Non-member Entities

Effective 15th Nov 2007 non-Client entities providing services to Visa Clients will be classified as;

- *Third Party:* A non-client that is not directly connected to VisaNet and provides payment-related services, directly or indirectly, to a Visa Client
- *VisaNet Processor:* A Client or non-Client that is directly connected to VisaNet and provides Authorization, Clearing, Settlement, or payment-related processing services for Merchants or Clients.
- New terminology does not apply to :
  - Co-branding partners
  - Card manufacturers
  - Card personalizers
  - Internet Payment Service Providers (IPSPs)

Visa's responsibilities

Enforce compliance via regional AIS programme

Manages communications, education, and support for Clients, merchants, third parties and Visanet processors.

Review and sign-off Report of Compliance for Clients, merchants, third parties and Visanet processors.

Works with Visa Clients to ensure compliance of their merchants, third parties and Visanet processors.

Client's responsibilities

All Clients must comply with the PCI Data Security Standard

Clients are responsible for ensuring the compliance of their merchants, third parties and Visanet processors who store, process, or transmit cardholder data

Ensure their merchants, third parties and Visanet processors do not store track data post authorization.

Report any data breach to Visa and take the appropriate action to mitigate further damage to the business and the Visa brand

Undergo compliance validation as outlined within the regional AIS programme

Any liability that may occur as a result of non-compliance with PCI DSS

Benefits of the AIS Programme

Benefits of the AIS Programme

Limits risk associated with data compromise and fraud

Improves confidence in the payment industry

Protects reputation

Promote brand Integrity

Boost consumer confidence

Provides competitive edge

Compliance Validation, Requirements and process

Compliance Validation, Requirements and process

Clients responsibilities

Merchant Levels Defined

Cemea VBV Mandate

Visanet processor and third party Levels Defined

Clients levels Defined

Compliance Validation Cycle

Compliance validation process

Who can validate compliance

Compensating controls

Other related requirements

Clients responsibilities

Clients are responsible for:

Registering with Visa all their Visanet processors and third parties

Ensuring their merchants, third parties and Visanet processors are PCI DSS compliant

Managing merchants, third parties and Visanet processors' communications

Clients responsibilities

Working with their merchants, third parties and Visanet processors until full compliance has been validated

Merchants, third parties and Visanet processors are not compliant until all requirements have been met and validated.

Responsible for providing Visa their merchants, third parties and Visanet processors' compliance status.

Merchant Levels Defined

Merchant level	Description	Validation required	Deadline
1	Any merchant regardless of acceptance channel processing over 6,000,000 Visa transactions per year.	(1) Annual on-site audit (2) Quarterly network scan	31st Dec 2007
2	Any merchant who is not a Level 1 and process, store or transmit 150,000 up to 6,000,000 Visa transactions per year.	(1) Annual self assessment questionnaire (2) Quarterly network scan	31st Dec 2007
3	Any merchant who is not a Level 1 and process, store or transmit up to 150,000 Visa transactions per year	(1) Annual self assessment questionnaire	31st Dec 2007

Only merchants who have the ability to store, process or transmit data need to be validated

Acquirers Responsibility

Identify and inform Visa of all there Level 1/2/3 merchants

Ensure their merchants validate compliance

Attest to Visa that their Level 1 merchants do not store track data

Ensure their e-commerce merchants are compliant to CEMEA Regional VBV mandate

Where there is a multi acquirer arrangement, the acquirer with the largest volume to take responsibility for the merchant's compliance

VBV Mandate

E-commerce merchants are not allowed to process payment in Cemea region.

Exceptions are granted to certain type of e-commerce merchants on a case by case basis.

Acquirers need to seek approval from Visa’s senior management prior to allowing merchants to store data.

Visa Processor and Third Party Levels Defined

Levels	Description	Validation required	Deadline
1	All VisaNet processors (member and non-member) and all payment gateways Any third party that stores, processes, or transmits more than 600,000 Visa transactions annually.	(1) Annual on-site audit (2) Quarterly network scan	31st Dec 2007
2	Any third party that stores, processes, or transmits 120,000 up to 600,000 Visa transactions annually.	(1) Annual self Assessment (2) Quarterly network scan	31st Dec 2007
3	Any third party that stores, processes, or transmits fewer than 120, 000 Visa transactions annually.	(1) Annual Self assessment Questionnaire	31st Dec 2007

Direct Connect Clients Levels Defined

Level	Threshold	Validation Requirement
1	Clients who process, store or transmit 600,000 or more Visa transactions annually	1. Annual on-site validation 2. Quarterly vulnerability scan
2	Clients who process, store or transmit 120,000 up to 600,000 Visa transactions annually	1. Annual self assessment 2. Quarterly vulnerability scan
3	Clients who process, store or transmit fewer than 120,000 Visa transactions annually	1. Annual self assessment

Deadline 31st Dec 2008

Changes to Validation requirements

Visa is in the process of reviewing validation requirements for merchants, service providers and direct connect clients.

New validation requirements to be published soon.

Validation Cycle

All entities must validate compliance on an annual basis.

Annual revalidation is required within 12 months from date of previous Report of Compliance was accepted

Quarterly scans must be performed at every three months interval or whenever the payment processing network is reconfigured.

Compliance Validation Process Merchants

Once the appropriate validation has been completed, the acquirer must provide Visa a Assertion Of Compliance letter indicating

- Name of merchant and type of validation completed
- Every requirement is met (including those met via compensating controls)
  - All remediation is complete and revalidated
- The PCI Security Audit Procedures were followed if an on-site review was performed.
- All findings are accurate
- No evidence of magnetic stripe data or CVV2 data storage

Compliance Validation Process – Third Parties, Visanet Processors and Direct Connect Clients

Third Parties, Visanet Processors and direct connect clients are required to undertake compliance validation independently by contracting the appropriate security vendor

Once the validation is completed, the security vendor and third party or Visanet processor must sign a Assertion Of Compliance letter indicating

- What validation task was completed
- Every requirement is marked “In Place” (including those met via compensating controls)
  - All remediation is complete and revalidated
- The PCI Security Audit Procedures were followed if an on-site was performed
- All findings are accurate
- No evidence of magnetic stripe data or CVV2 data storage

Who can validate compliance?

On-site review must be performed by a PCI SSC approved Qualified Security Assessor (QSA)

Self assessment – Ideally must be performed by an internal IT auditor or a QSA to ensure impartiality and accuracy.

Vulnerability scanning must be performed by a PCI SSC approved Scan Vendor (ASV)

List of approved QSA and ASV can be found on:

https://www.pcisecuritystandards.org

Other related requirements

- PCI PIN Security Standard

Clear PIN and PIN Block must not be stored in transaction journal or logs post authorisation.

- International Member Letter 14/04

Effective 1st April 2007, PAN must be truncated in cardholder copy of receipt.

Effective 1st April 2005, all newly deployed devices must have the capability to truncate PAN

Useful contacts

Standard (PCI DSS, PA DSS and PCI PED), validation tools and approved vendors.

www.pcisecuritystandards.org./

Visa Cemea's AIS Programme Office

CEMEAAIS@visa.com

Free PCI DSS Training

http://www.parkli.com/VisaDS/

Reporting data breach

- Visa Regional Risk Head
- CemeaFraudcontrol@Visa.com

Payment Application Security

Mani Tulasi

Payment Security Risk (Cemea region)

November 2008

Agenda

- What is a Payment Application?
- Payment Application Best Practices
- Payment Application Data Security Standard
- Payment Application Security Mandates

What is a Payment Application?

- Any **third-party** payment application utilized by a merchant or agent that is involved in the authorization or settlement of a payment card transaction
- **IN SCOPE**: point of sale, middle-ware, shopping carts/store fronts, handheld devices, payment kiosks, ATMs
- **OUT OF SCOPE**: in-house use only developed applications, stand-alone POS terminals, database software, web server software
- Standalone POS terminals are out of scope only if **all** of the following are true:
  - The terminal has no connections to any of the merchant's systems or networks
  - The terminal connects to the acquirer or processor
  - The terminal vendor provides secure remote access, updates, maintenance and troubleshooting
  - The following are never stored post authorization: the full contents from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere), CVV, CVV2, PIN or encrypted PIN block

Payment Application Best Practices

Milestones in the adoption of secure payment applications

- Visa PABP launched in 2005 to eliminate the storage of prohibited data and facilitate PCI DSS compliance for merchants and agents
- List of validated payment applications published monthly since January 2006
  - As of 03/31/08, 296 payment applications across 130 vendors have been validated by a Qualified Security Assessor (QSA) *
- List of vulnerable payment applications published quarterly since April 2007

*** Statistic for the US region only**

Industry Collaboration

- Payment industry has developed PCI DSS to promote the protection of cardholder data
- PCI SSC, launched in September 2006, is a global forum for the ongoing development and enhancement of security standards for account data protection, including the PCI DSS
- PCI SSC announces adoption of Visa's PABP as the Payment Application Data Security Standard (PA-DSS)
- Visa, Amex, Discover, JCB and MasterCard founding members
- Responsible for certification and training for assessors and scan vendors
- Payment card industry stakeholders are invited to join as Participating Organizations and can be elected to an Advisory Board

Payment Application Data Security Standard

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

- **PCI SSC is responsible for:**
  - Maintaining and updating the PA-DSS standard and related documentation
  - Qualifying and training Payment Application Qualified Security Assessors (PA-QSAs) to perform PA-DSS reviews
  - Being a single point of repository for PA-DSS Reports of Validation (ROVs)
  - Performing Quality Assurance (QA) reviews of PA-DSS ROVs to confirm report consistency and quality
  - Listing PA-DSS validated payment applications on the PCI SSC website at www.pcisecuritystandards.org
- **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

PA-DSS Requirements

1) Do not retain full magnetic stripe or CVV2 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

Clients, Service Providers, merchants and vendors responsibilities

- Vendors
  - Payment application vendors must ensure their applications are validated for compliance by a PA –QSA
  - Work with PCI SSC to validate and list their compliance applications
- Clients
  - Verify against the PCI SSC listing and ensure they deploy only PA DSS compliant payment applications
  - Ensure their service providers and merchants deploy only PA DSS compliant payment applications
- Service providers and merchants
  - Verify against the PCI SSC listing and ensure their deploy only PA DSS compliant payment applications

Payment Application Security Mandates

Visa plans to aggressively drive the adoption of secure payment applications in the marketplace

Visa CEMEA to announce PA DSS mandates Oct 2008

Reference Tools

PCI Security Standards Council (PCI SSC)

- Data Security Standard
- Payment Application Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaire
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

www.pcisecuritystandards.org

Thank You!