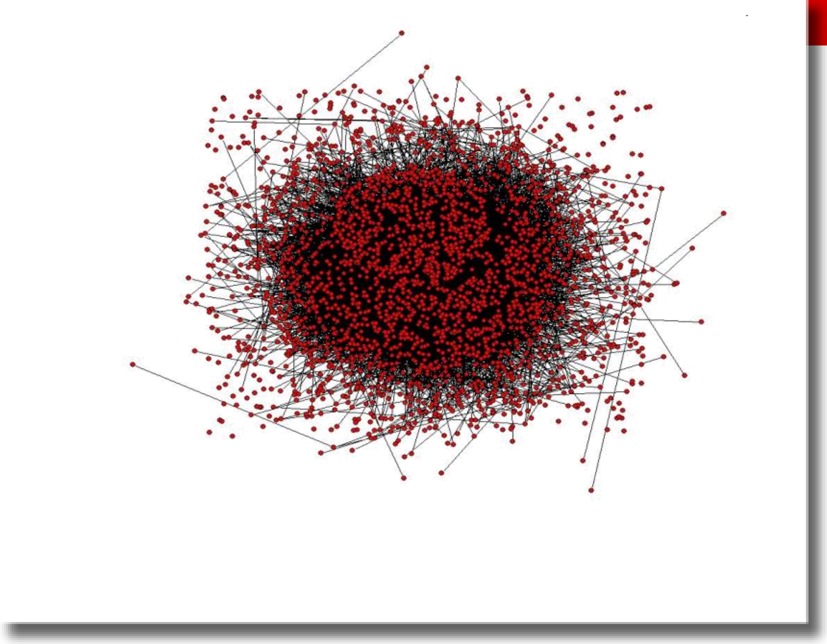
PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

PCI Security Standards Council™
APPROVED SCANNING VENDOR

PCI Security Standards Council™
PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR



# Implementation and assessment on cryptography for payment solutions

**Yan Liu ,** yan@atsec.com, atsec China

CISSP, ISO/IEC 27001 LA,

PCI QSA, PA DSS QSA, ASV

24 - 26 Sep 2013, ICMC, Gaithersburg

# Content

- Payment Card Industry (PCI) Standards and their relationship between FIPS 140-2 standard;
- The proposal on security implementation
- Testing methodology
- Conclusion

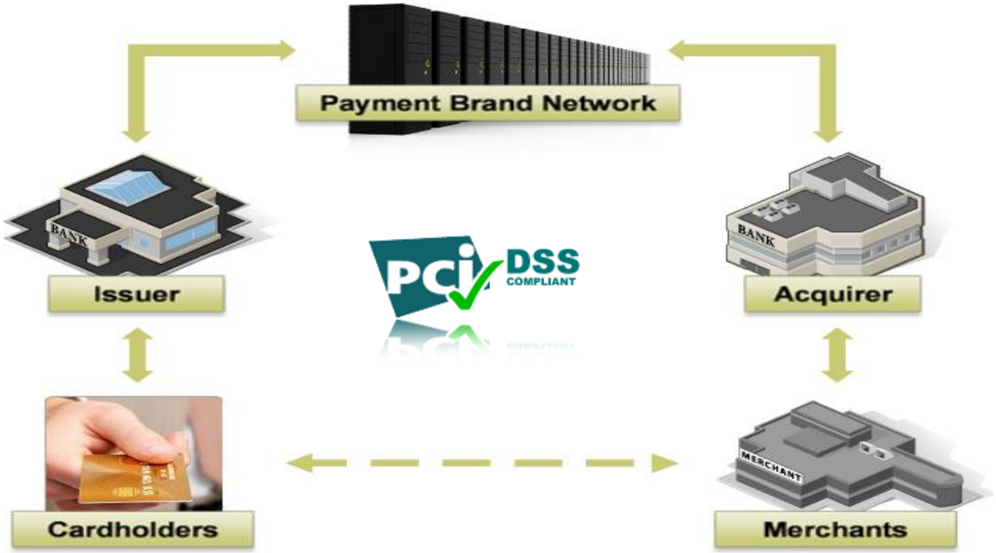
# Definition of "Strong Cryptography"

- *Cryptography based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Cryptography is  a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or “one way”).*
- *Examples of industry-tested and accepted standards and algorithms for encryption include AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher), and ElGamal (1024 bits and higher).*
- *See NIST Special Publication 800-57 (http://csrc.nist.gov/publications/) for more information.*

- The strong cryptography accepted by PCI industry includes but not limited to FIPS-approved algoirthms as mentioned above.

# Payment Card Industry and Its Related Roles

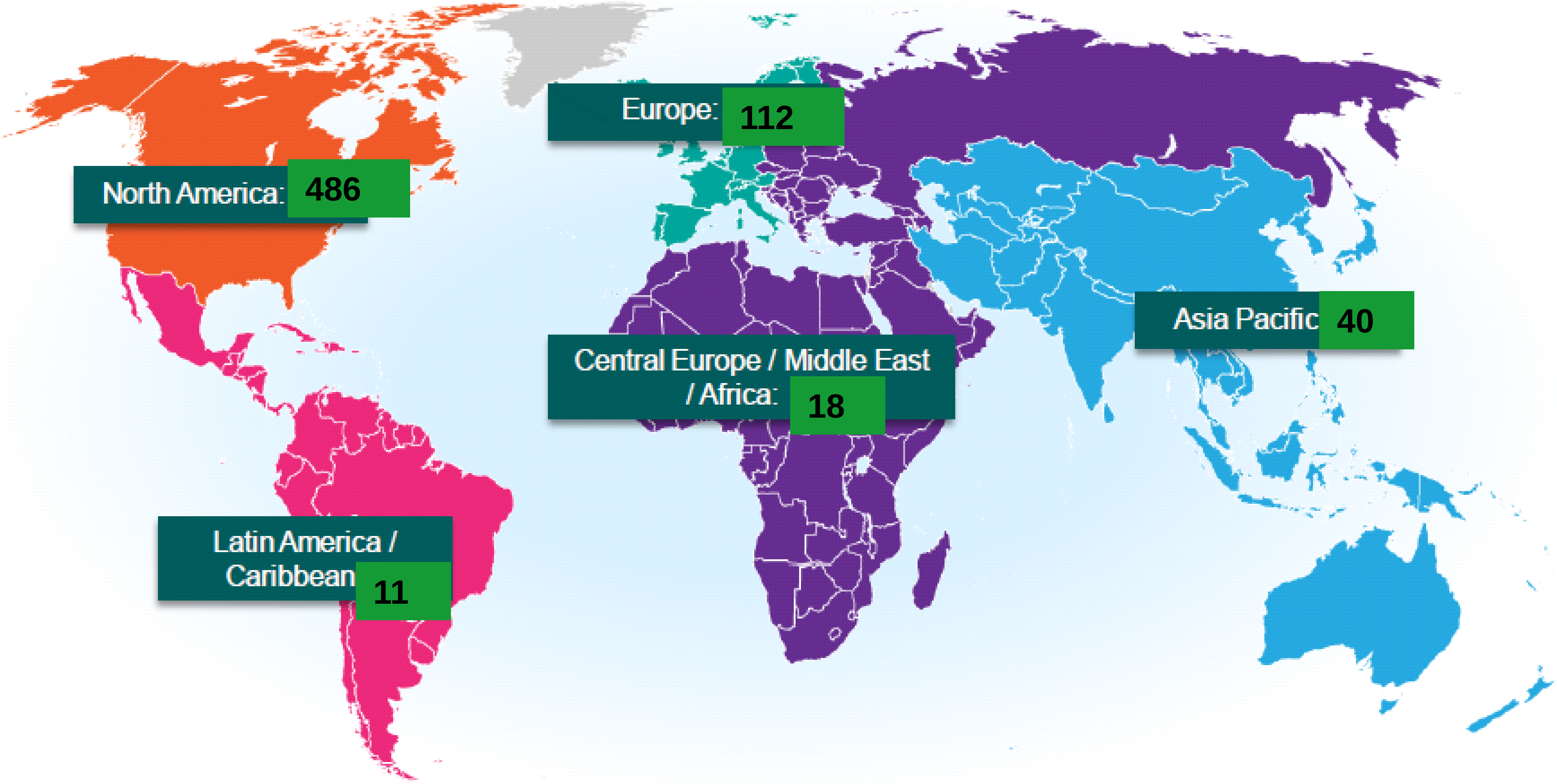
- PCI (Payment Card Industry)
- PCI  roles
  - Cardholders
  - Issuers
  - Merchants
  - Acquirers
  - Payment or Card Brands
  - Service Providers



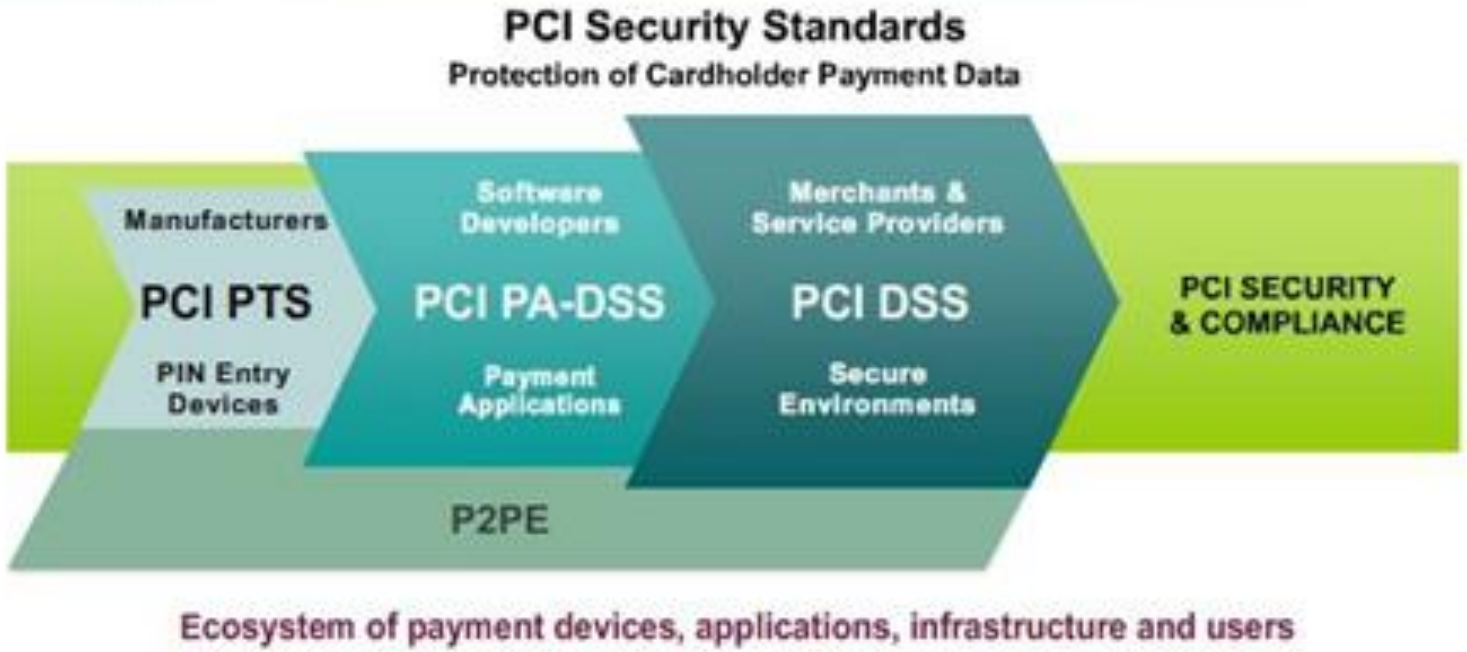
- Payment processing
  - Authorization
  - Clearing
  - Settlement

# PCI Participating Organizations globally

679 organizations are participating until 25 Aug 2013


Europe: 112
North America: 486
Asia Pacific 40
Central Europe / Middle East / Africa: 18
Latin America / Caribbean 11

# Key PCI Standards


PCI Security Standards
Protection of Cardholder Payment Data
Manufacturers
PCI PTS
PIN Entry Devices
Software Developers
PCI PA-DSS
Payment Applications
Merchants & Service Providers
PCI DSS
Secure Environments
PCI SECURITY & COMPLIANCE
P2PE
Ecosystem of payment devices, applications, infrastructure and users

***June 2013:** **C**ard Production Logical and Physical Security Requirements (new)

Information Source from PCI SSC

# Previous SIG

## Virtualization

PCI DSS Virtualization Guidelines Jun 2011

## Mobile

Mobile Payment Security Guidelines, Sep 2012

## Encryption

Point-to-Point Encryption Technology and PCI DSS Compliance

P2PE standard (released in 2012) contains security requirements and testing procedures for application vendors and providers to ensure the data protection.

## Wireless

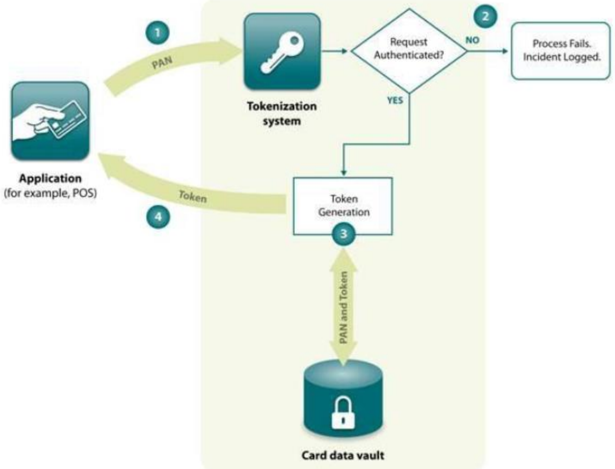
PCI DSS 2.0 Wireless Guidelines Aug 2011

## EMV

PCI DSS Applicability in an EMV Environment Oct 2010

## Tokenization

PCI DSS Tokenization Guidelines, Aug 2011



# Recent SIG

Cloud

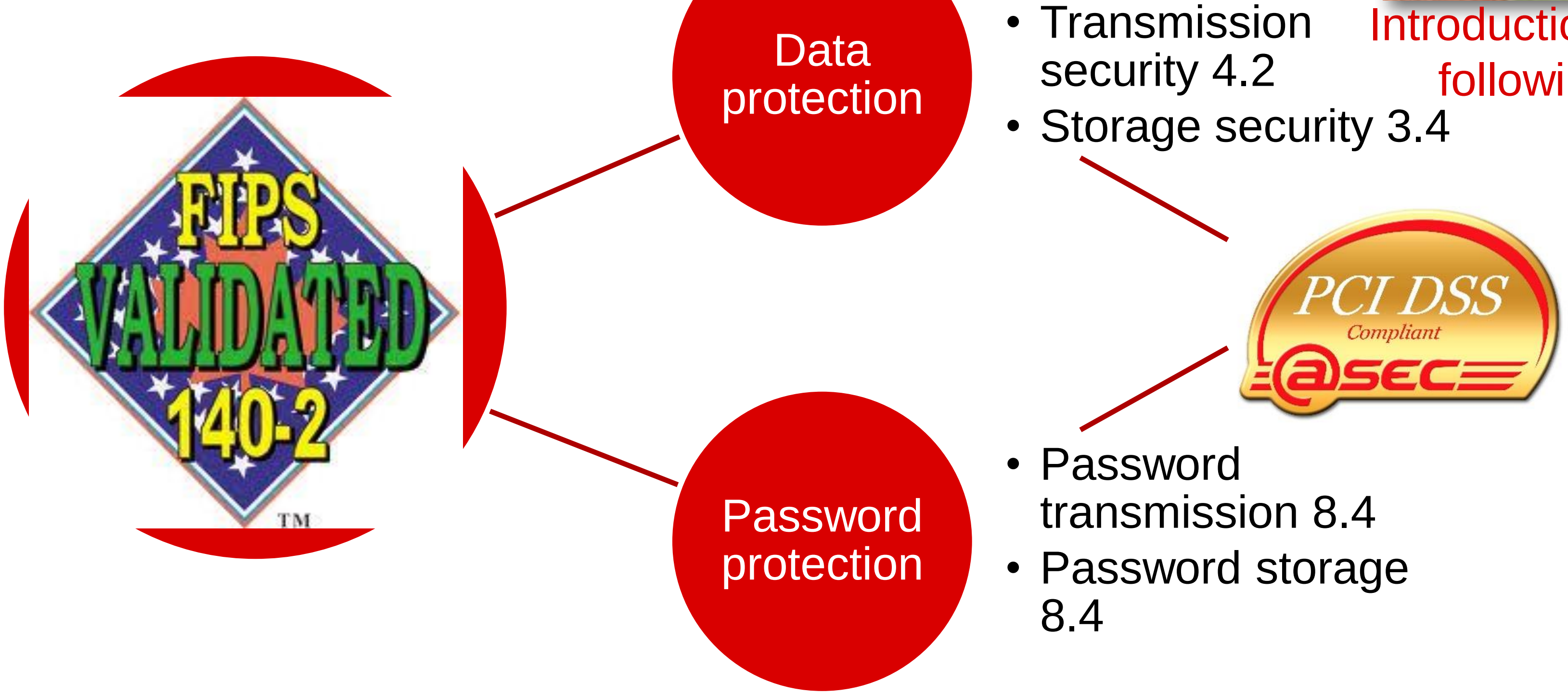
E-commerce security

Risk assessment

Nov 2012, PCI DSS Risk Assessment Guidelines v1.0

Third Party Security Assurance, plan to be done in 2013
Best Practices for Maintaining PCI DSS Compliance, plan to be done in 2014
Proposed SIG: Penetration testing scoping, by atsec, securitymetrics, and paysw.

# FIPS 140-2 vs PCI



Data protection

- Transmission security 4.2
- Storage security 3.4

Introduction in following slides

Password protection

- Password transmission 8.4
- Password storage 8.4

PCI DSS requirement 8.4 mentioned that “Render all passwords unreadable during transmission and storage on all system components using strong cryptography.”

# PCI DSS basic requirement

## Storage of payment card information

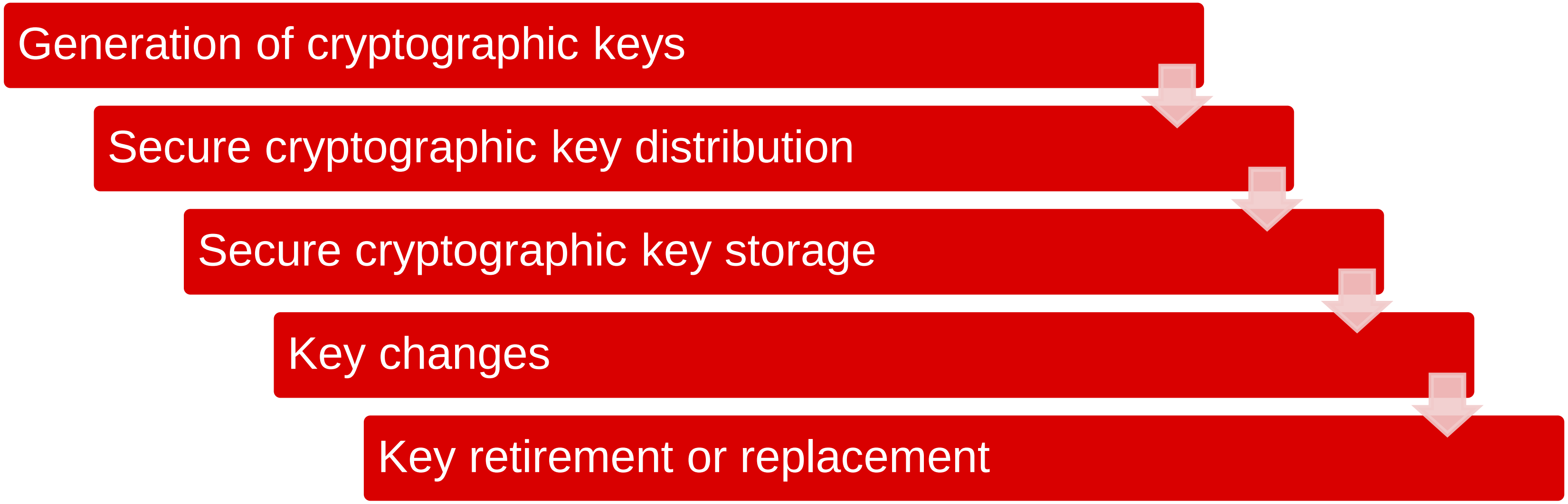
| Storage of Card Data | | | | |
|---|---|---|---|---|
| | **Data Element** | **Storage permitted** | **Protection Required** | **PCI DSS Req 3.4** |
| **Cardholder Data** | Primary Account Number (PAN) | √ | √ | √ |
| | Cardholder Name | √ | √ | ☒ |
| | Service Code | √ | √ | ☒ |
| | Expiration Date | √ | √ | ☒ |
| **Sensitive Authentic-ation Data** | Full Magnetic strips | ☒ | | |
| | CVC2/CVV CID/CAV2 | ☒ | | |
| | PIN/PIN Block | ☒ | | |

# Protection of cardholder data

- Requirement 3.4 mentioned the approaches to render PAN unreadable, including:
  - One-way hashes based on strong cryptography,
  - Truncation,
  - Index tokens and pads,
  - Strong cryptography with associated key management.
- PCI DSS Tokenization Guideline was released in Aug 2011.
- PCI DSS requirement 3.4.1 mentioned regarding disk encryption, the logical access must be managed independently of native operating system access control mechanisms, and decryption keys must not be tied to user accounts.

# Key management

- PCI DSS requirement 3.5 mentioned the protection of cryptographic keys against disclosure and misuse (access control and secure storage)
- PCI DSS 3.6 mentioned key management, including:



Generation of cryptographic keys

Secure cryptographic key distribution

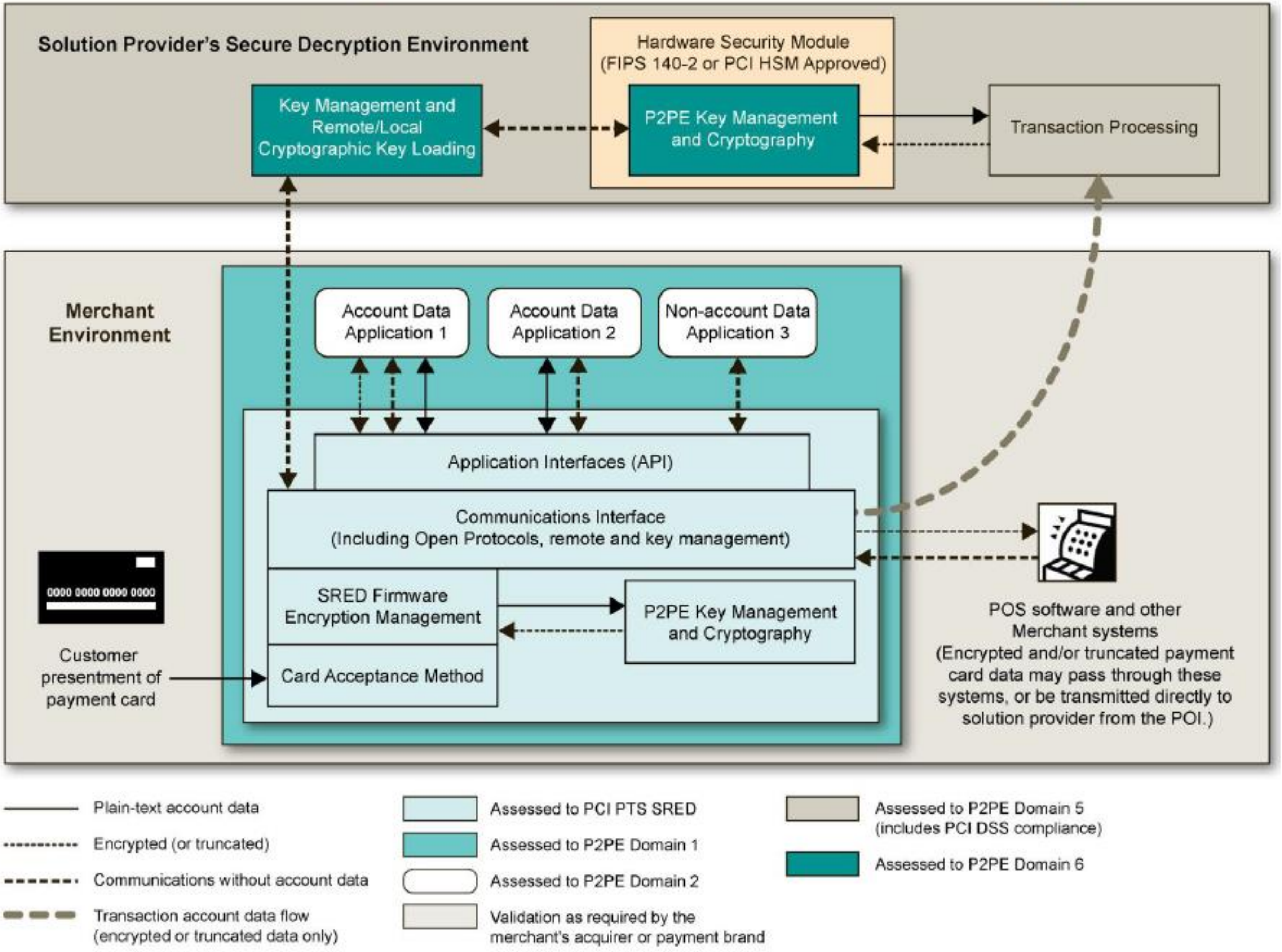
Secure cryptographic key storage

Key changes

Key retirement or replacement

  - Split knowledge and dual control for manual clear-text cryptographic key
  - Prevention of unauthorized subsitution of keys, and also the formal acknowledge for key custodians.

# Glance – Illustration of a typical P2PE Implementation and Associated Requirements



Solution Provider's Secure Decryption Environment

Hardware Security Module (FIPS 140-2 or PCI HSM Approved)

Key Management and Remote/Local Cryptographic Key Loading

P2PE Key Management and Cryptography

Transaction Processing

Merchant Environment

Account Data Application 1

Account Data Application 2

Non-account Data Application 3

Application Interfaces (API)

Communications Interface (Including Open Protocols, remote and key management)

SRED Firmware Encryption Management

P2PE Key Management and Cryptography

Card Acceptance Method

Customer presentment of payment card

POS software and other Merchant systems (Encrypted and/or truncated payment card data may pass through these systems, or be transmitted directly to solution provider from the POI.)

—— Plain-text account data

········ Encrypted (or truncated)

- - - - Communications without account data

▬ ▬ ▬ Transaction account data flow (encrypted or truncated data only)

▭ Assessed to PCI PTS SRED

▭ Assessed to P2PE Domain 1

▭ Assessed to P2PE Domain 2

▭ Validation as required by the merchant's acquirer or payment brand

▭ Assessed to P2PE Domain 5 (includes PCI DSS compliance)

■ Assessed to P2PE Domain 6

# Protection of CHD transmission

- PCI DSS requirement 4.1 mentioned that “Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, for instance:
  - The Internet
  - Wireless technologies
  - Global System for Mobile communications (GSM)
  - General Packet Radio Service (GPRS)

# Similar requirements in PA DSS

- The PA DSS applies to 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.
- PA DSS requirement 2.3 alignes with PCI DSS req 3.4;
- PA DSS requirement 2.5 alignes with PCI DSS req 3.5;
- PA DSS requirement 2.6 alignes with PCI DSS req 3.6;
- PA DSS requirement 11.1 alignes with PCI DSS req 4.1;
- PA DSS requirement 3.3 alignes with PCI DSS req 8.4.

# General crypto solutions

## Encryption hardware

- Hardware cost: Medium
- Maintenance cost: Low

## Database encryption

- Software cost: High
- Maintenance cost: Medium

## Application write into database

- Application development cost: High
- Maintenance cost: Medium

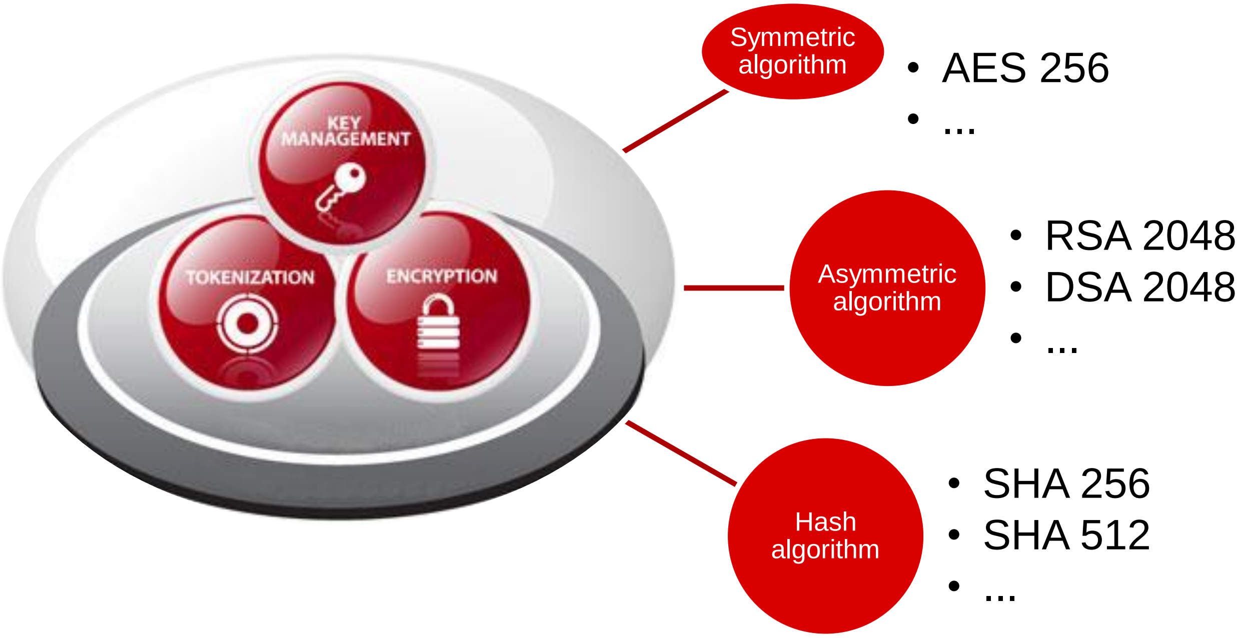
## File/disk encryption

Software cost: Medium

Maintenance cost: High

# Proposed crypto solution

- Crypto solutions are proposed by atsec QSA by combining best practice of the industry and working experience with payment organizations including acquiring banks, issuing bank, payment service providers, merchants during recent years.
  The key used for encrypting cardholder data should be securely protected, for instance by using a Key encryption key.



Symmetric algorithm

- AES 256
- ...

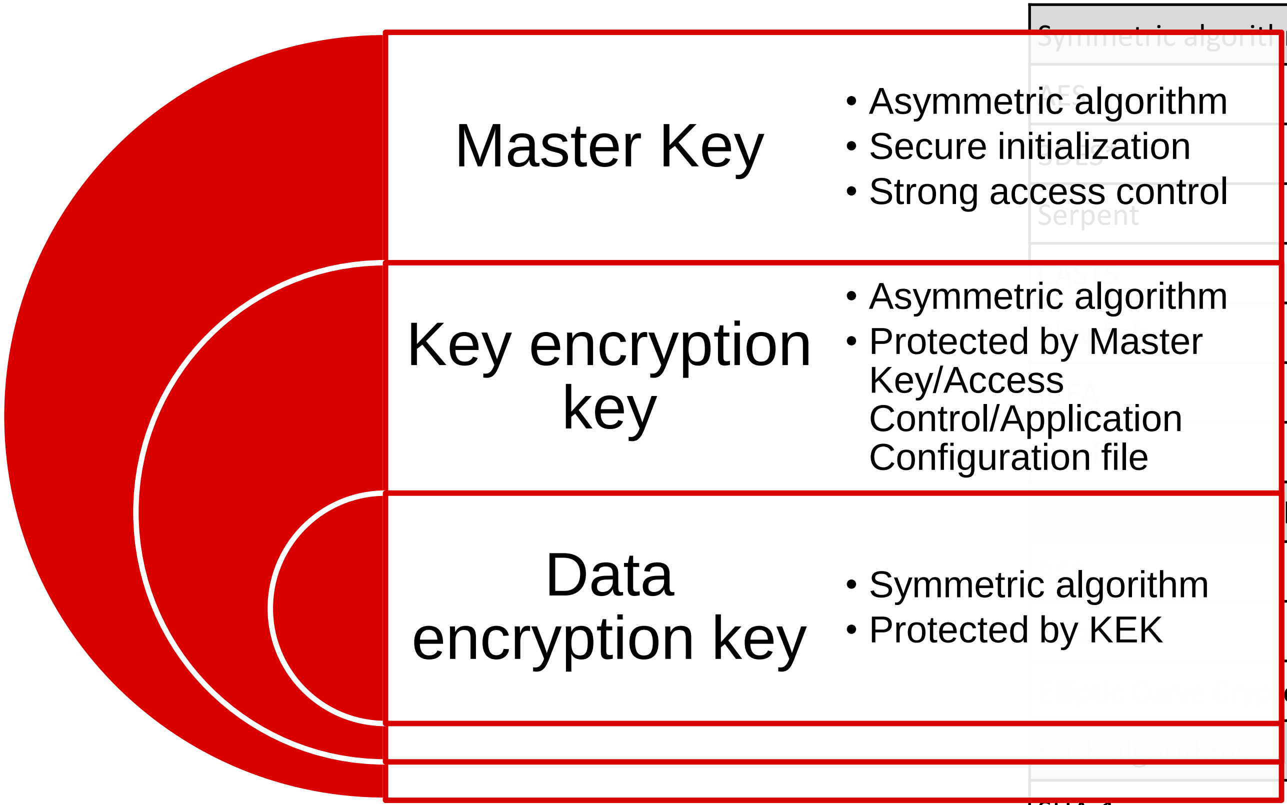
Asymmetric algorithm

- RSA 2048
- DSA 2048
- ...

Hash algorithm

- SHA 256
- SHA 512
- ...

# Proposed keys system



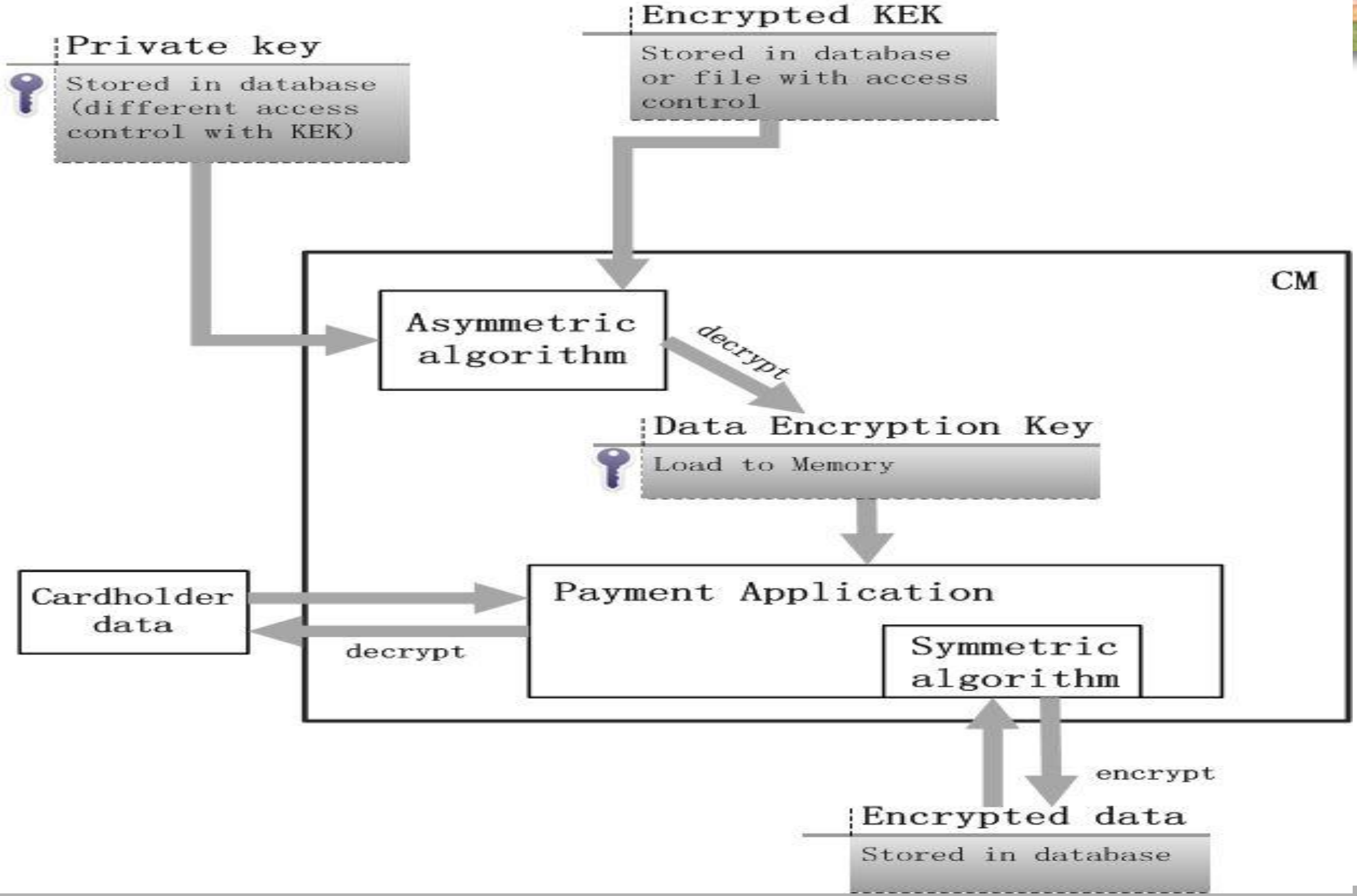
Master Key
- Asymmetric algorithm
- Secure initialization
- Strong access control

Key encryption key
- Asymmetric algorithm
- Protected by Master Key/Access Control/Application Configuration file

Data encryption key
- Symmetric algorithm
- Protected by KEK

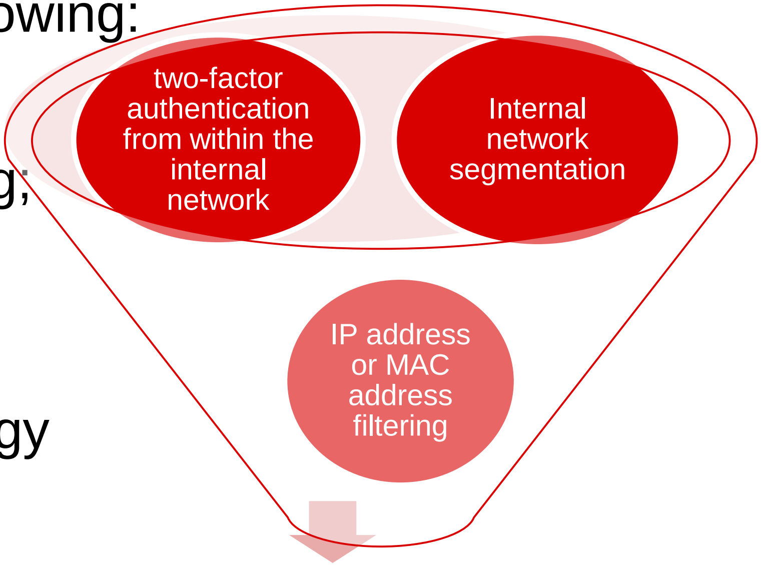
| Symmetric algorithms | Size |
|---|---|
| AES | 256 |
| 3DES* | 128 |
| Serpent | 256 |
| CAST5 | 128 |
| Blowfish | 448 |
| IDEA | 128 |
| Twofish | 128 |
| Asymmetric algorithms | |
| RSA | 2048 |
| DSA | 2048 |
| Elliptic Curve Cryptosystem* | 192 |
| Hash algorithms | |
| SHA-1 | 256 |
| RIPE-MD | 160 |

# Proposed encryption solution with 2 keys



# Proposed compensating control

- The compensation control could be accepted if data encryption can not be implemented in the system, e.g. banks which implmented a cardholder data environment many years ago.
- The control should address all of the following:
  - (1) internal network segmentation;
  - (2) IP address or MAC address filtering;
  - and (3) two-factor authentication from within the internal network
- In addition to above-mentioned technology implementation, the implementation on policy and procedure is also important, e.g. the key management process.


two-factor authentication from within the internal network
Internal network segmentation
IP address or MAC address filtering

Compensating Control

# Summary of req 3.4: protection of cardholder data

| Protection Mechanism | If CHD after the protection | Business affect | Applicability description |
|---|---|---|---|
| Masked PAN | No | High | When the business requirement can be accepted. |
| Hash | No | High | When the business requirement can be accepted. |
| Tokenization | No | Medium | When the business requirement can be accepted. |
| Strong encryption | Yes | Low | When full PAN is needed. |
| Compensating control | Yes | Low | When full PAN is needed, and strong encryption is not possible. |

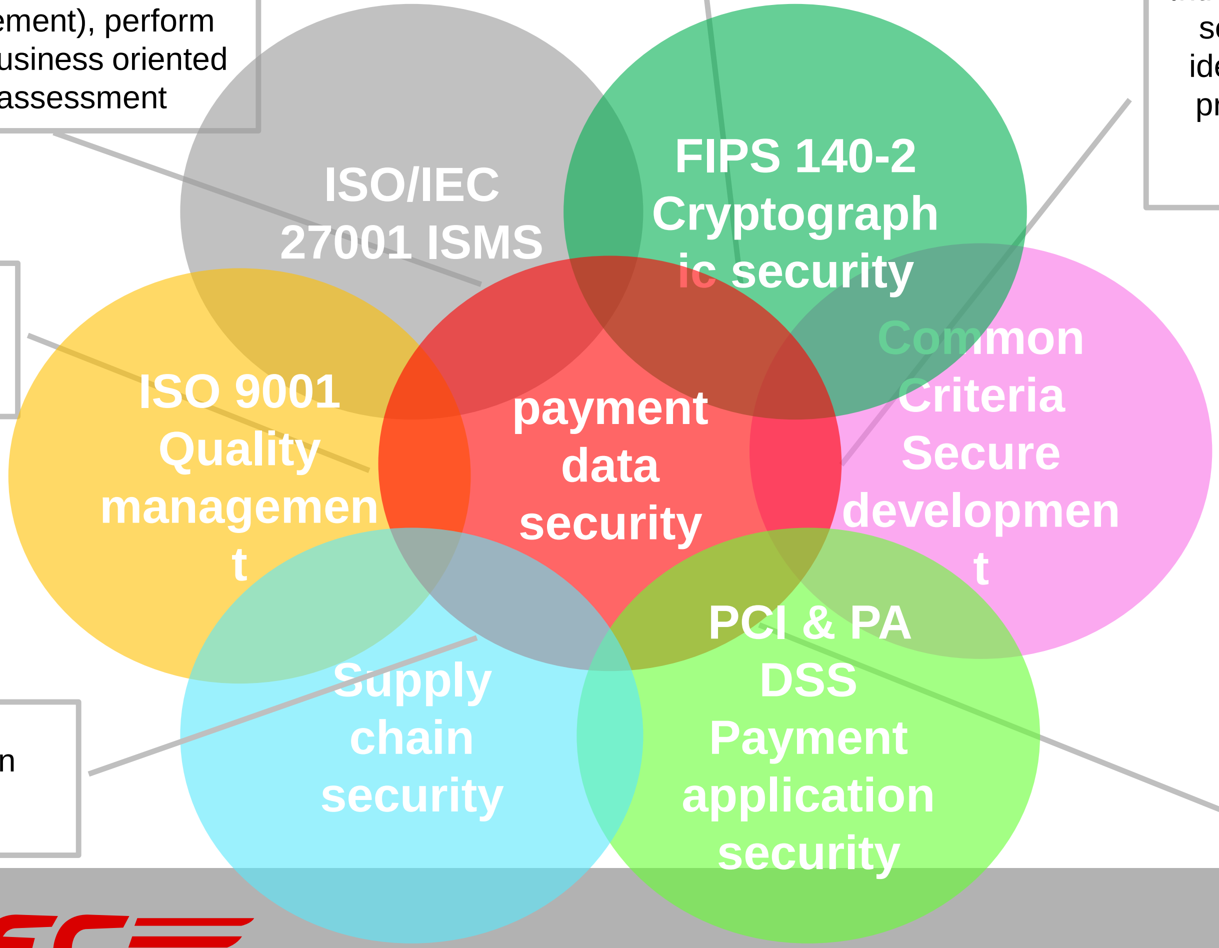
# atsec methodology: Integrated and unified Management System

Establish common management system (Configuration Management), perform assets/business oriented risk assessment

The use of cryptographic algorithms
Key Management

Introducing CC standard secure development idea, risk assessment process and also the idea of PP

Improve quality management



ISO/IEC 27001 ISMS

FIPS 140-2 Cryptograph ic security

ISO 9001 Quality managemen t

payment data security

Common Criteria Secure developmen t

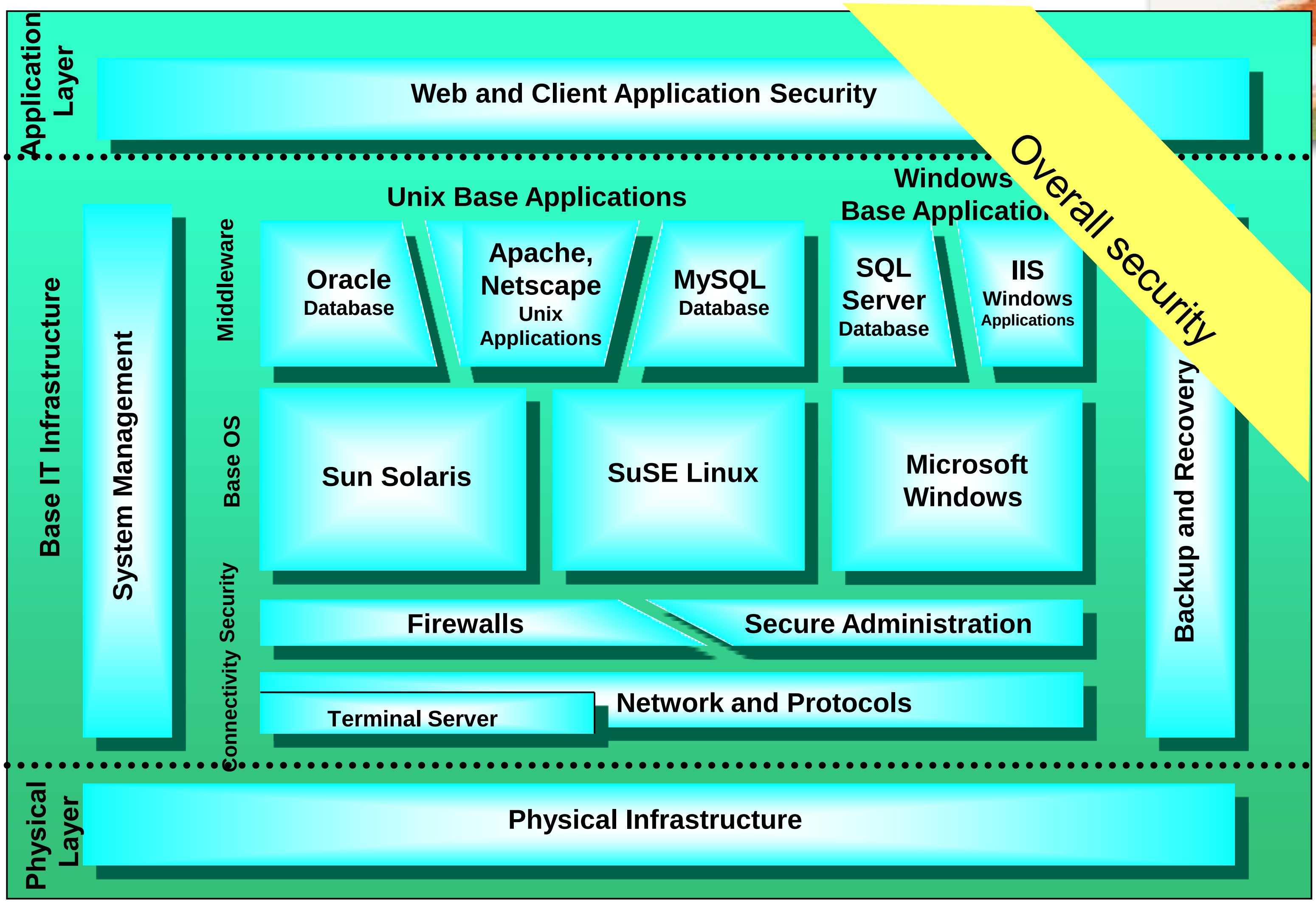
Supply chain security

PCI & PA DSS Payment application security

Supply chain security

PCI DSS and PA DSS to protect cardholder and sensitive data

# IT Base Infrastructure

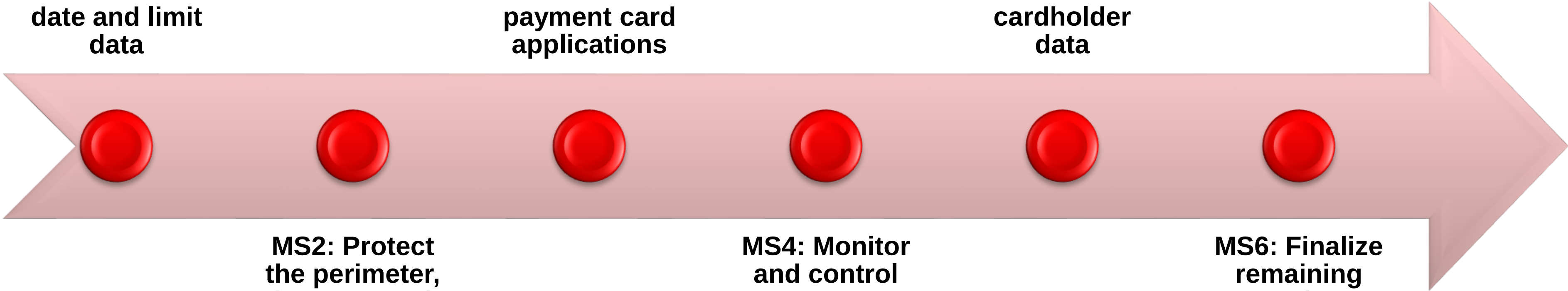


Idea source from atsec Germany

# Other key points on Physical and Network Security

- PCI DSS as a best practice.
- Sensitive data should be encrypted using industry-standard methods when stored on disk or transmitted over public networks.
- Cryptographic protocols (such as SSL v3.0) for data transmission; the website and interface are accessible via certificates issued by authorized parties.
- Strong cryptographic algorithms and well-design and implemented key management (FIPS 140-2 could be considered during the implementation)
- Installs security updates and patches on all system components.
- Security hardening, settings of applications and devices are tuned to ensure appropriate levels of protection.
- Networks are strictly segregated and strong access controls are in place, e.g. restrictive firewalls protect all connections between networks.
- Audit management and security monitor
- Authentication: password complexity, two-factor authentication for remote access, etc.
- Physical security

# Prioritized Approach



**MS1: Remove sensitive authentication date and limit data**

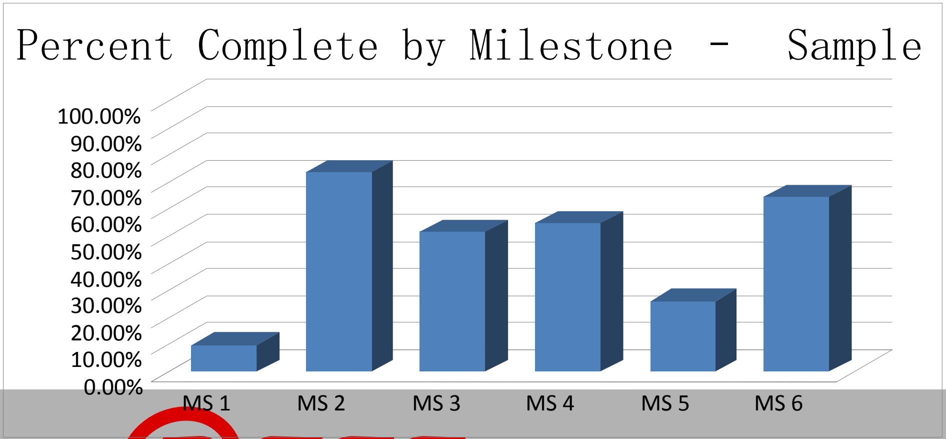
**MS2: Protect the perimeter, internal, and wireless networks**

**MS3: Secure payment card applications**

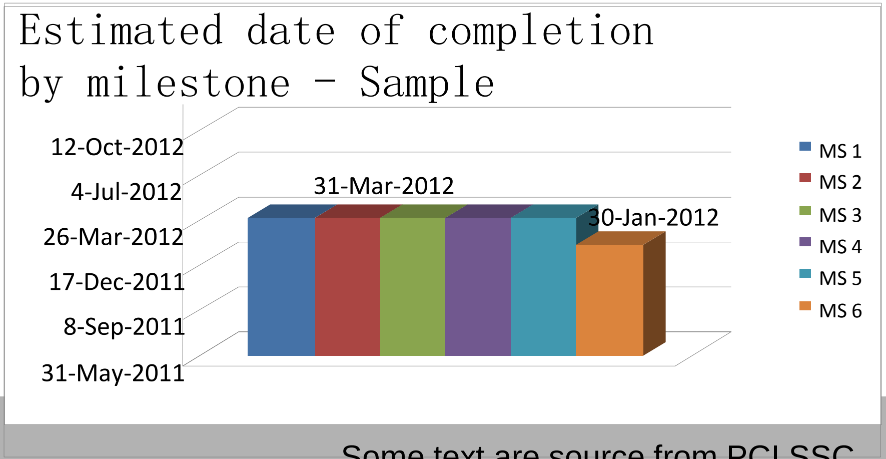
**MS4: Monitor and control access to your systems**

**MS5: Protect stored cardholder data**

**MS6: Finalize remaining compliance efforts, and ensure all controls are in place**



Percent Complete by Milestone - Sample



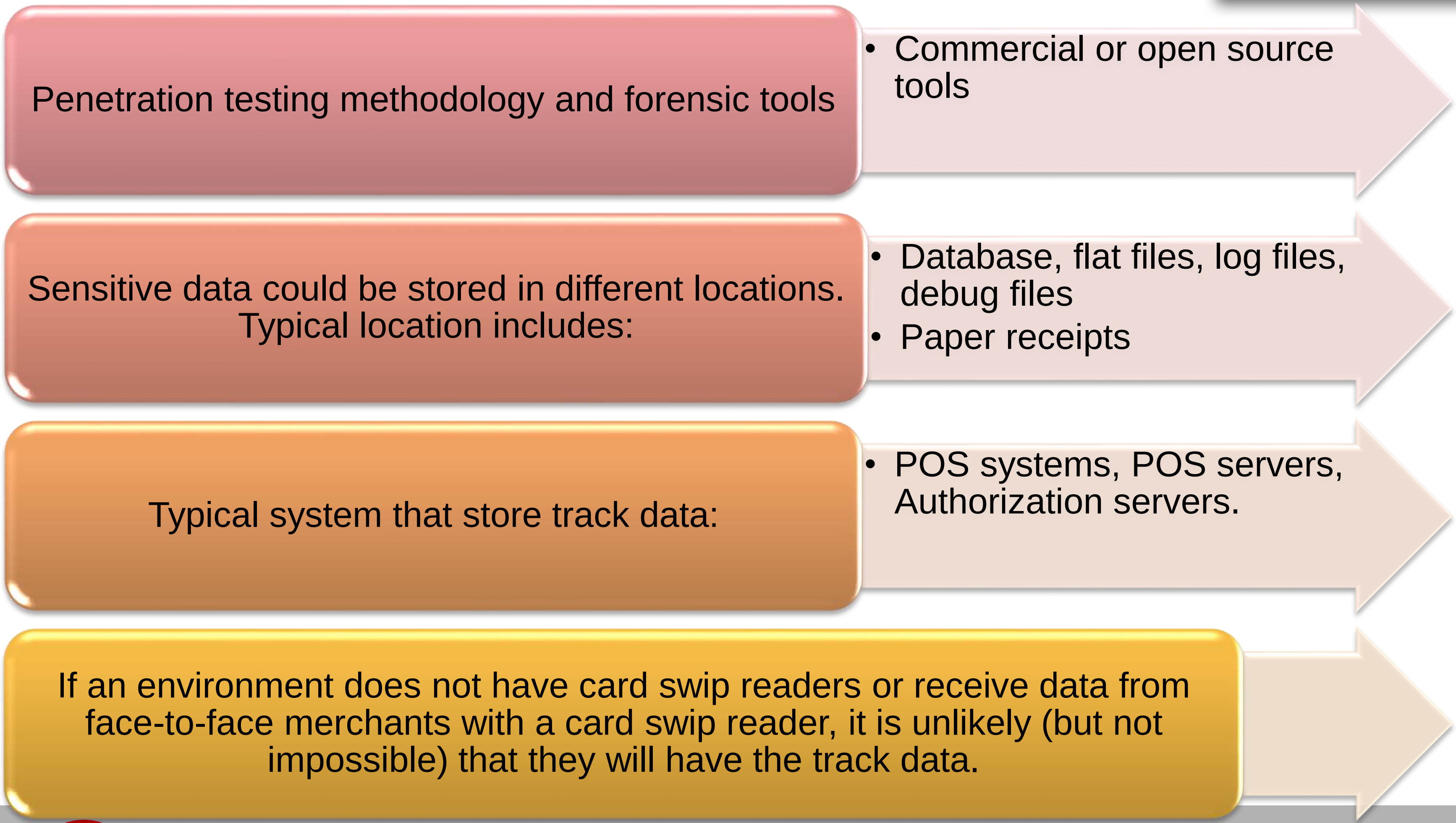
Estimated date of completion by milestone - Sample

Some text are source from PCI SSC

# Testing methodology

- It would be recommended for payment organization and/or payment vendors to achieve FIPS 140-2 certification for the implmented cryptographic algorithms and/or modules, in order to simplify the testing effort during the PCI assessment.
- The methodology and tools used for the testing, especially examine "clear-text" sensitive data on potential locations like transaction message, history, log, trace, and debug files, database schemas and contents.
- Automatic tool and manual examination should be combined for the whole forensic process because of the payment dataflow.

# Sensitive Data Discovery



Penetration testing methodology and forensic tools

- Commercial or open source tools

Sensitive data could be stored in different locations. Typical location includes:

- Database, flat files, log files, debug files
- Paper receipts

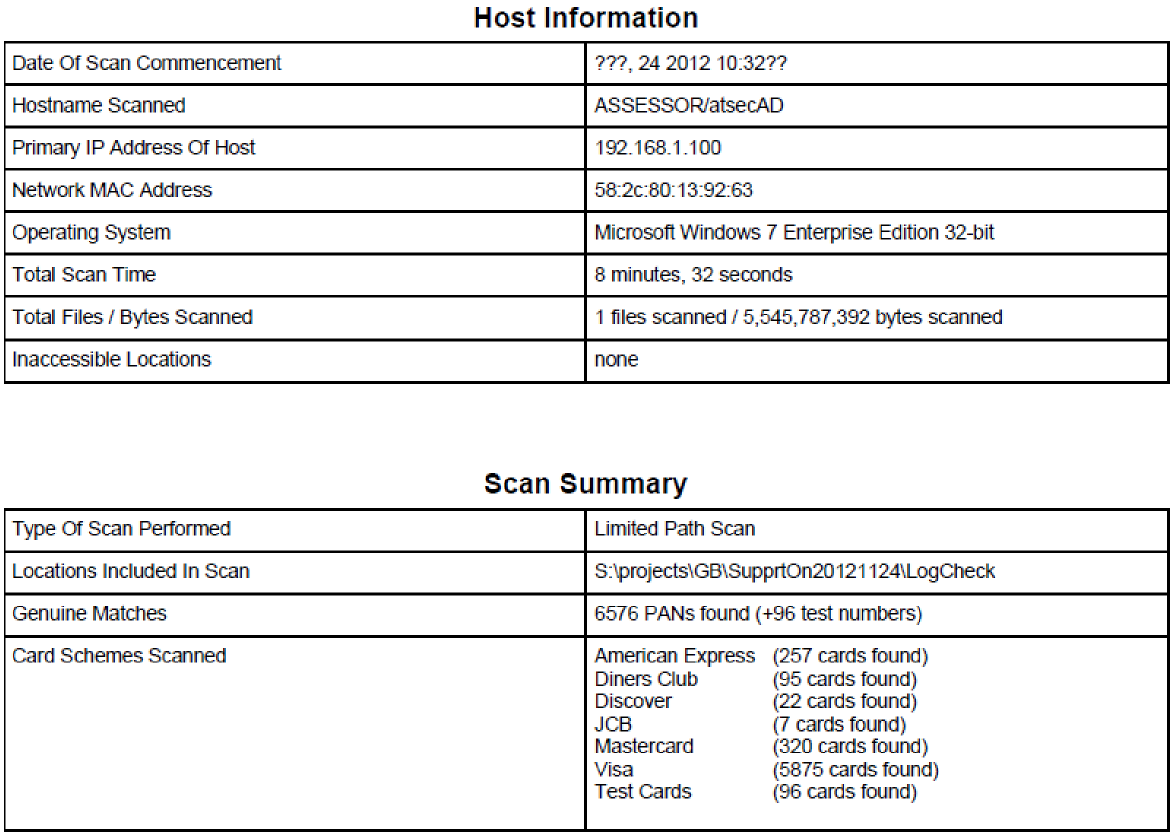
Typical system that store track data:

- POS systems, POS servers, Authorization servers.

If an environment does not have card swip readers or receive data from face-to-face merchants with a card swip reader, it is unlikely (but not impossible) that they will have the track data.

# Example of CHD discovery

- Card Recon
- Spider 2008

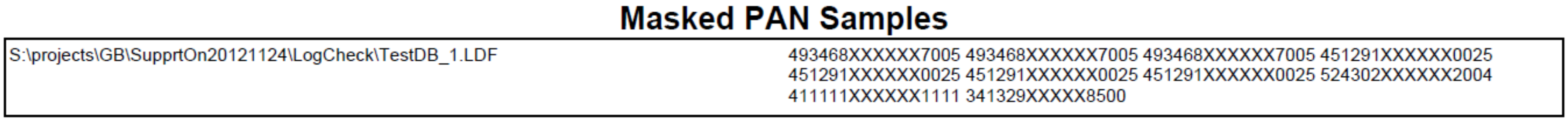


### Host Information

| | |
|---|---|
| Date Of Scan Commencement | ???, 24 2012 10:32?? |
| Hostname Scanned | ASSESSOR/atsecAD |
| Primary IP Address Of Host | 192.168.1.100 |
| Network MAC Address | 58:2c:80:13:92:63 |
| Operating System | Microsoft Windows 7 Enterprise Edition 32-bit |
| Total Scan Time | 8 minutes, 32 seconds |
| Total Files / Bytes Scanned | 1 files scanned / 5,545,787,392 bytes scanned |
| Inaccessible Locations | none |

### Scan Summary

| | |
|---|---|
| Type Of Scan Performed | Limited Path Scan |
| Locations Included In Scan | S:\projects\GB\SupprtOn20121124\LogCheck |
| Genuine Matches | 6576 PANs found (+96 test numbers) |
| Card Schemes Scanned | American Express (257 cards found)<br>Diners Club (95 cards found)<br>Discover (22 cards found)<br>JCB (7 cards found)<br>Mastercard (320 cards found)<br>Visa (5875 cards found)<br>Test Cards (96 cards found) |



### Masked PAN Samples

| | |
|---|---|
| S:\projects\GB\SupprtOn20121124\LogCheck\TestDB_1.LDF | 493468XXXXXX7005 493468XXXXXX7005 493468XXXXXX7005 451291XXXXXX0025 451291XXXXXX0025 451291XXXXXX0025 451291XXXXXX0025 524302XXXXXX2004 411111XXXXXX1111 341329XXXXX8500 |

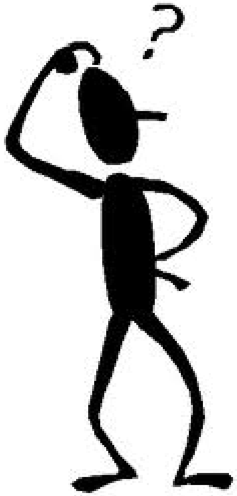
# Conclusion

- The security implemenmtation on cryptography for payment solutions cover the technology areas data encryption and decryption, key management, password protection, and also related IT processes.
- A standards-combined approach is used for the overall security proposal including standards like FIPS 140 (cryptographic module and key management), PCI DSS, PA DSS (payment industry best practice), CC (introduced security development and risk management methodology), etc.
- Various technical expertise and services are required for data protection, including encryption/key management, hash, tokenization, etc.

# Conclusion – cont.

- Security monitor, security architecture, large scale risk assessment, penetration testing, and in-depth security analysis are also reqeusted in order to verify the implmentation.
- Independent security audit, testing and evaluation are important, nevertheless different validation requirements could be considered for different security levels.

# Resources



- https://www.pcisecuritystandards.org/
  - – PCI standards and related documents
  - – QSA、ASV、PA QSA、PFI qualification maintenance

- http://www.atsec.com/

QUALIFIED SECURITY ASSESSOR

APPROVED SCANNING VENDOR

PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR