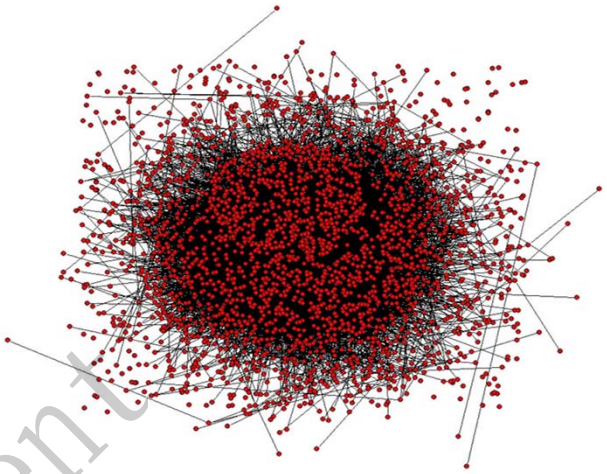


支付安全实践分享

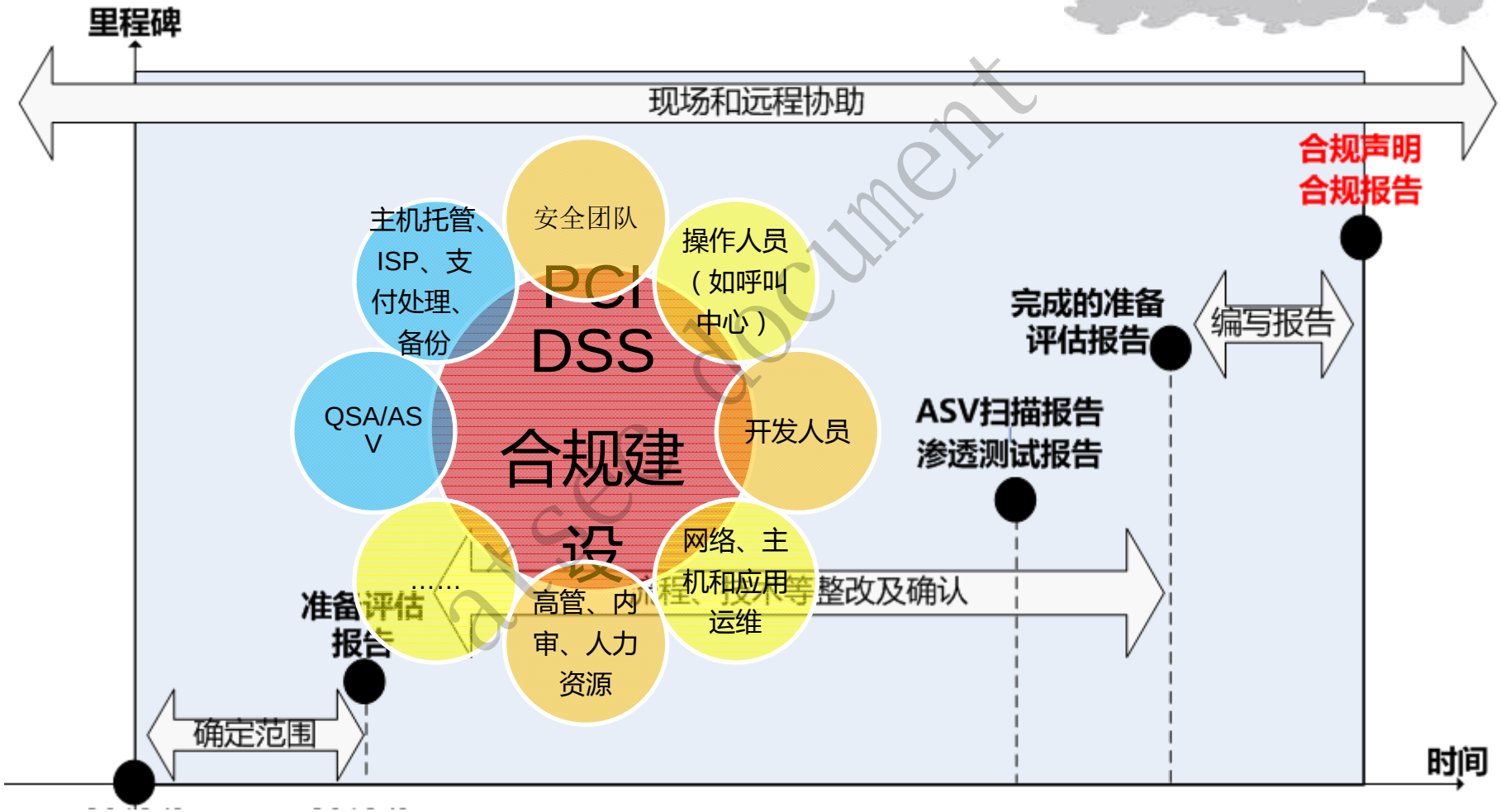
2014年2月28日, 中国 北京

Yan Liu , yan@atsec.com, atsec China

CISSP, ISO/IEC 27001 LA, O-TTPS

PCI QSA, PA DSS QSA, ASV

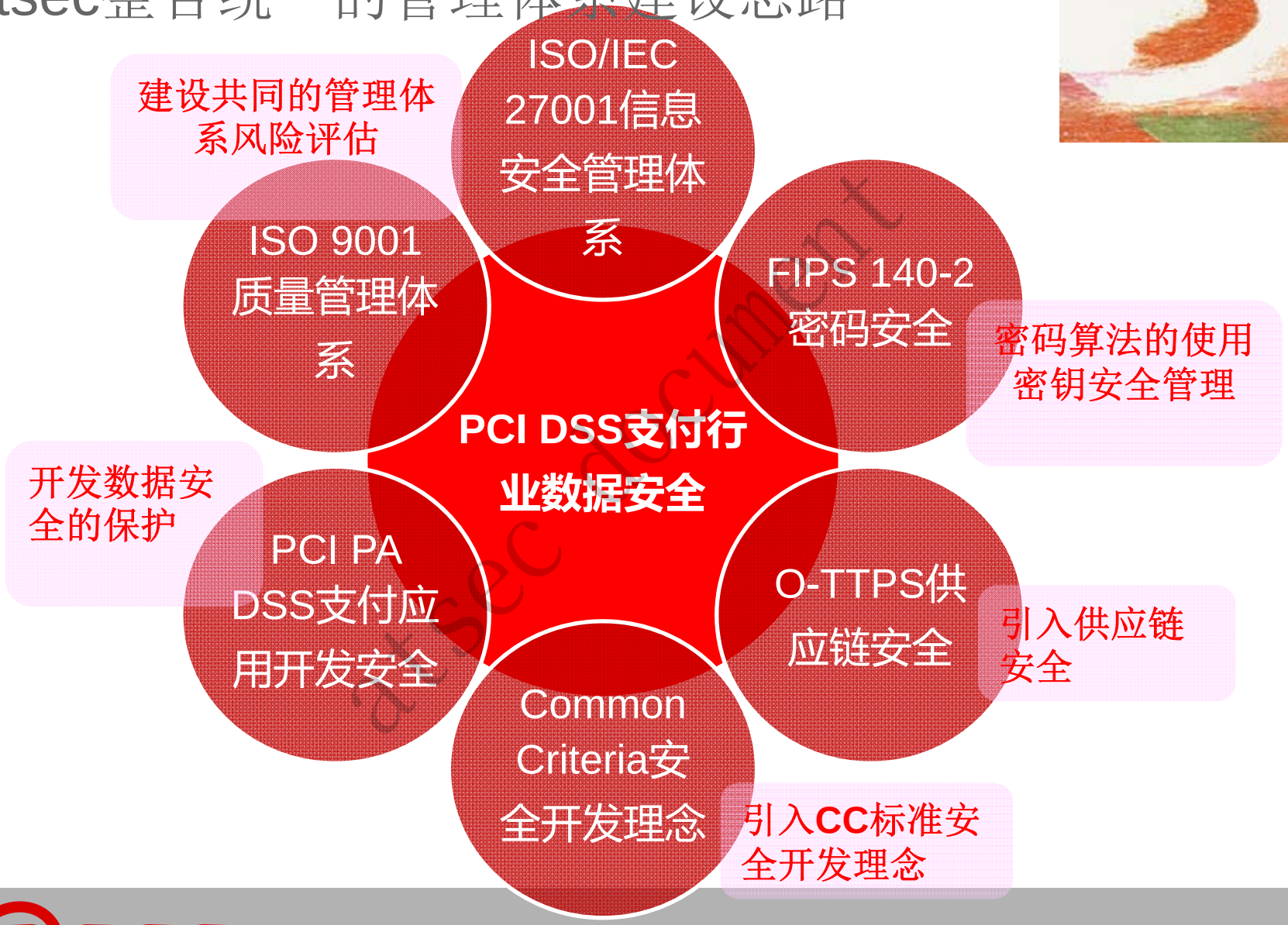
PCI DSS合规建设思路分享



最佳实践重点分享：

- **整合统一的信息安全管理体系**
- **密码实现**
- **合规与测试**

atsec整合统一的管理体系建设思路



PCI与ISMS整合的组织安全和管理体系实例

蓝色代表整合体系文档

红色代表PCI体系文档

黑色代表原体系文档

O 组织和办公	B 业务相关制度	I IT管理	Q 质量管理	S 安全管理

一级文件（管理办法）

管理体系管理办法	网络架构安全管理办法	物理和办公环境安全管理办法	加密机制管理办法	设计和开发安全管理办法	安全测试管理办法	变更控制管理办法	日志安全管理指引	持卡人数据保护管理办法	访问控制安全管理办法	网络安全管理办法	防病毒管理办法	账号和口令管理办法	漏洞及脆弱性管理办法	日志管理办法	岗位与职责描述	第三方管理规范	信息资产管理办法	信息交换和介质安全管理办法

一级文件（操作指引）

支付业务描述	人力资源操作指引	文件和记录管控办法	安全编码规范	信息安全培训操作指引	信息安全风险评估操作指引	应急响应操作指引	系统配置操作指引	介质管理的操作指引	信息资产管理的操作指引	变更控制管理流程	帐号安全管理指引	授权管理操作指引	日志安全管理指引	漏洞安全管理指引	物理和办公环境安全操作指引	第三方安全管理操作指引	管理评审操作指引	软件开发安全管理指引	防火墙配置标准	防病毒操作指引	漏洞评价	软件安全需求评估

最佳实践重点分享：

- **整合统一的信息安全管理体系**
- **密码实现**
- **合规与测试**

PCI DSS根本要求

- 信用卡数据存储 适用性信息

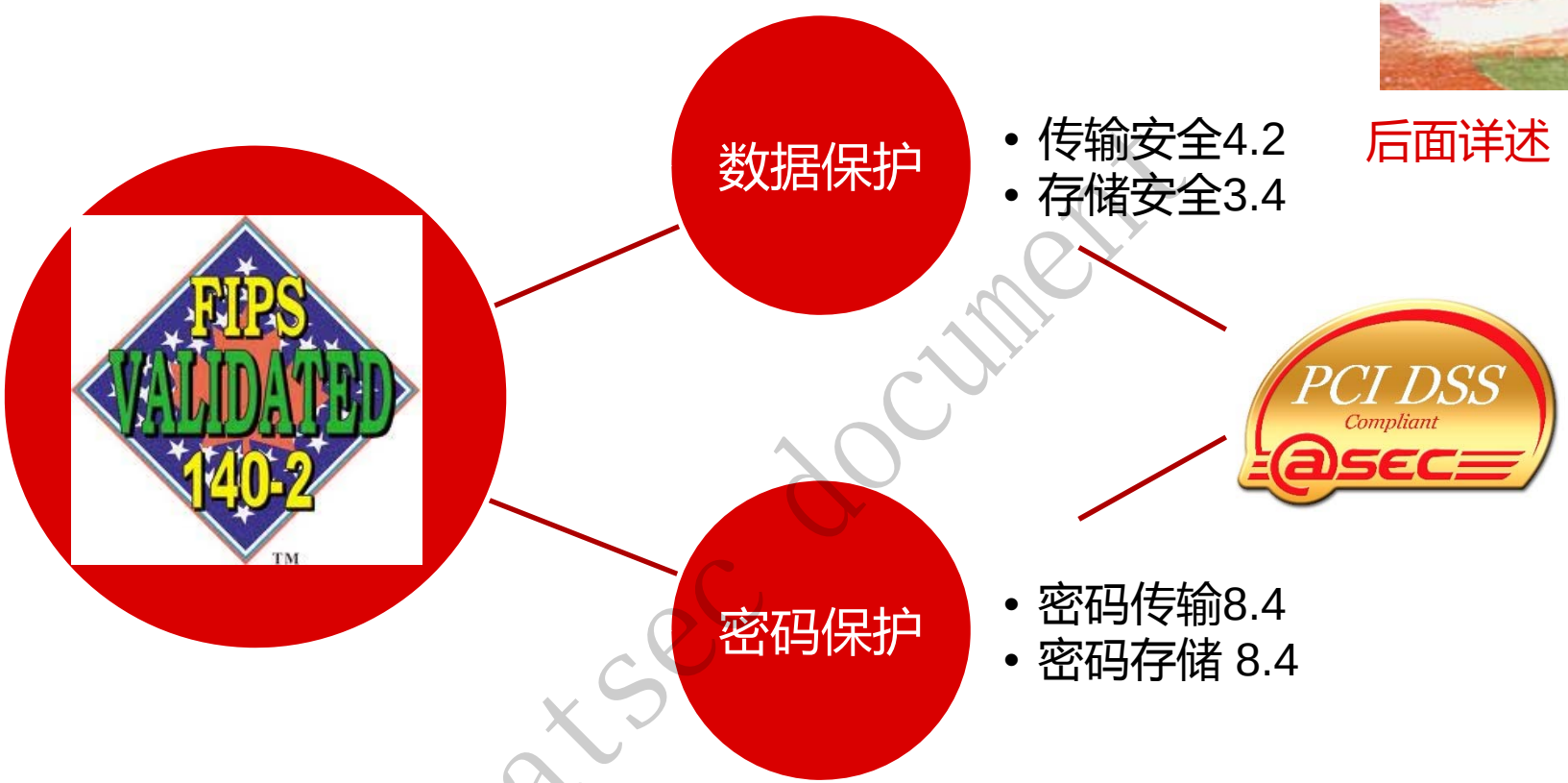
持卡人数据的存储 **Storage of Card Data**				
	Data Element	**Storage permitted**	**Protection Required**	**PCI DSS Req 3.4**
Cardholder Data 持卡人数据	Primary Account Number (PAN)	√	√	√
	Cardholder Name	√	√	☒
	Service Code	√	√	☒
	Expiration Date	√	√	☒
Sensitive Authentic-ation Data 敏感的认证数据	Full Magnetic strips	☒		
	CVC2/CVV CID/CAV2	☒		
	PIN/PIN Block	☒		

PCI标准关于强加密的定义

- *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.*

- 支付产业认可的强加密包括但不限于FIPS认可的算法（上述提及）

FIPS 140-2 vs PCI



PCI DSS 要求8.4 “采用强加密，呈现在所以系统组件上的所有密码在传输和存储时不可读。”

存储数据的保护

- 要求3.4提及如下方法确保数据不可读：
  - One-way hashes based on strong cryptography,
  - Truncation,
  - Index tokens and pads,
  - Strong cryptography with associated key management.
- PCI DSS Tokenization Guideline，Aug 2011发布
- PCI DSS要求3.4.1 提及关于硬盘加密：the logical access must be managed independently of native operating system access control mechanisms, and decryption keys must not be tied to user accounts.

密钥管理

- PCI DSS 要求3.5 提及密钥保护，防止泄露和误用（访问控制和安全存储）
- PCI DSS 3.6 提及密钥管理，包括：
  - **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.

数据传输的保护

- PCI DSS 要求4.1 提及 “使用强加密和安全协议，比如SSL/TLS, IPSEC, SSH, 等，保护在公共开放网络上传输的敏感持卡人数据，公共开放网络包括但不限于：
  - The Internet
  - Wireless technologies
  - Global System for Mobile communications (GSM)
  - General Packet Radio Service (GPRS)

通常加密解决方案

加密机

- 硬件成本：Medium
- 维护成本：Low

数据库加密

- 软件成本：High
- 维护成本：Medium

应用程序

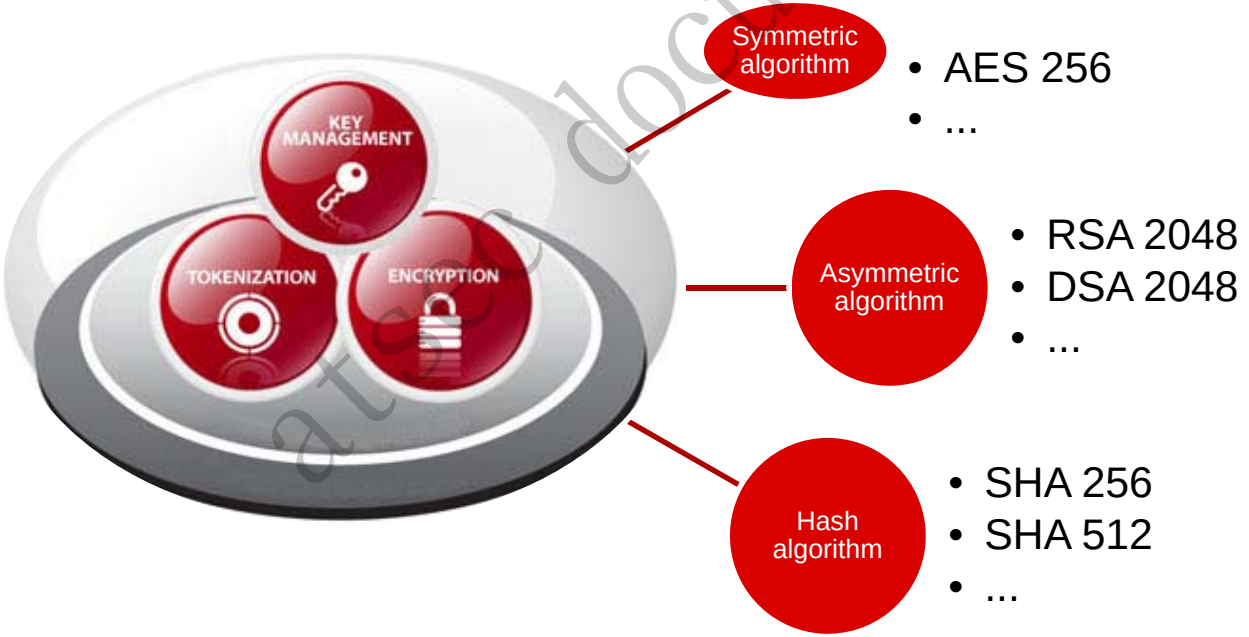
- 应用开发成本：High
- 维护成本：Medium

文件/磁盘加密

- 软件成本：Medium
- 维护成本：High

加密解决方案建议

- atsec结合与诸多支付机构（包括银行、支付机构、商户）多年工作，结合产业实践，提出加密解决方案建议。
  用于加密数据的密钥应保证足够安全，比如使用密钥加密密钥进行保护。



建议的密钥体系

主密钥
Master Key

- Asymmetric algorithm
- Secure initialization
- Strong access control

密钥加密密钥
Key encryption key

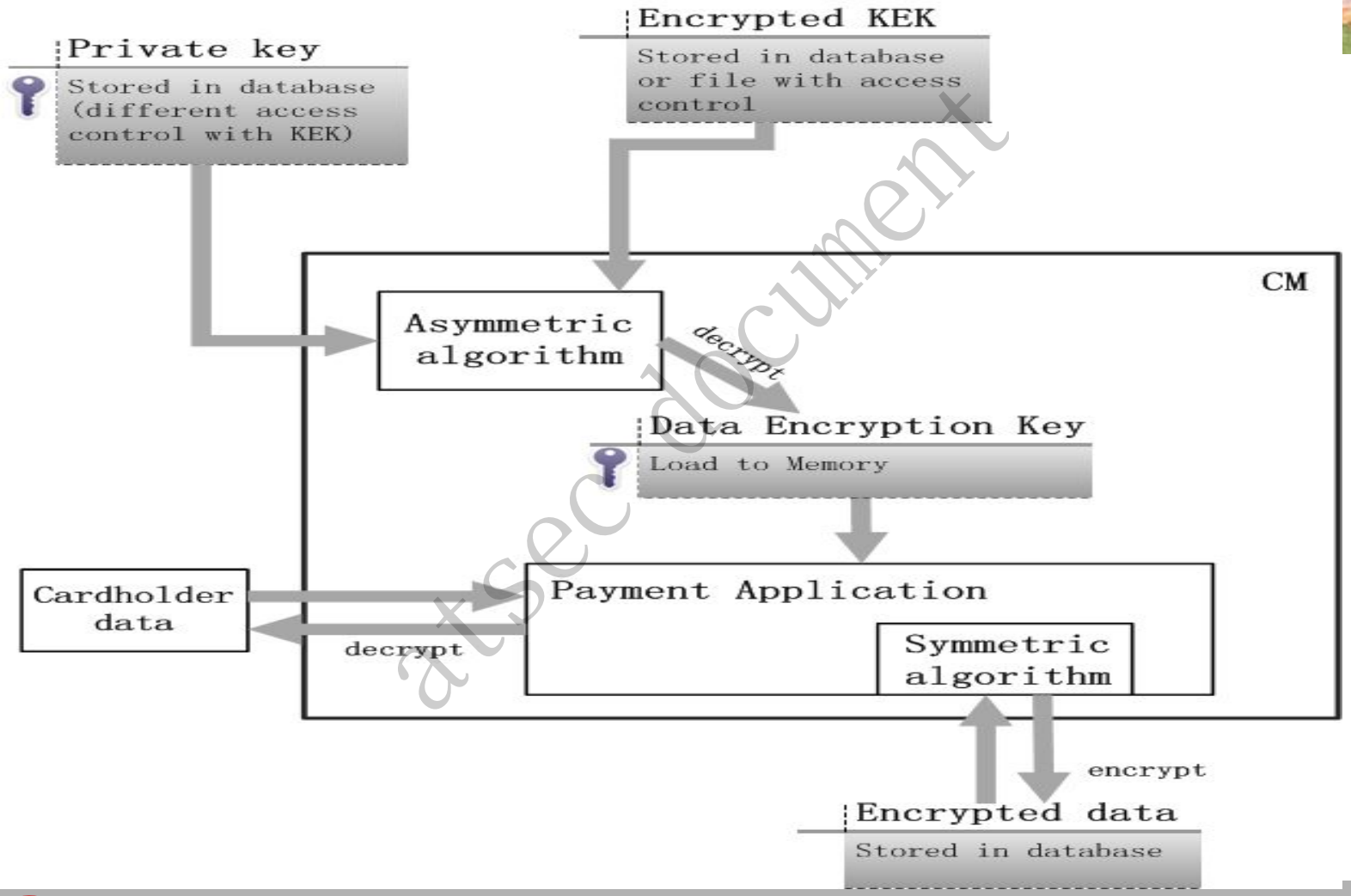
- Asymmetric algorithm
- Protected by Master Key/Access Control/Application Configuration file

数据加密密钥
Data encryption key

- Symmetric algorithm
- Protected by KEK

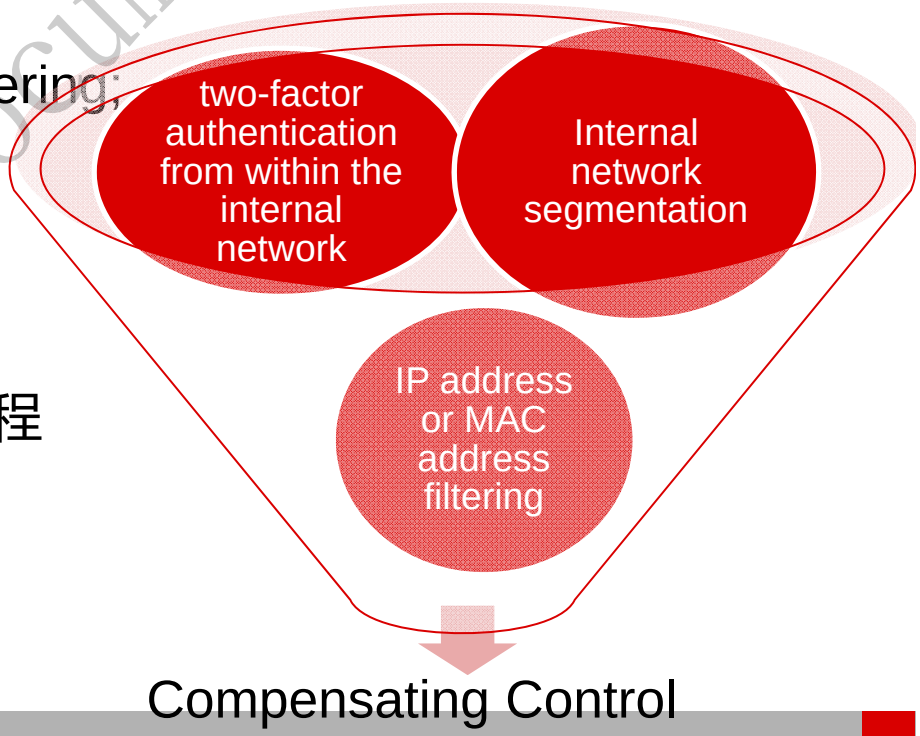
Symmetric algorithms	Size
AES	256
3DES*	128
Serpent	256
CAST5	128
Blowfish	448
IDEA	128
Twofish	128
Asymmetric algorithms	
RSA	2048
ElGamal	2048
Elliptic Curve Cryptosystem*	192
Hash algorithms	
SHA-1	256
RIPE-MD	160

建议的两层密钥加密解决方案



可以参考的补偿控制措施

- 补偿控制可能被QSA所讨论和接受，如果系统中的数据加密由于限制无法实现，比如银行所实现持卡人数据环境多年暂时不能实现加密。
- 可以考虑的补偿控制如下（同时满足）：
  - (1) internal network segmentation;
  - (2) IP address or MAC address filtering;
  - (3) two-factor authentication from within the internal network
- 此外，上述技术实现所涉及的
- 策略和流程同样重要，如密钥管理过程
- 补偿控制需要定期审核



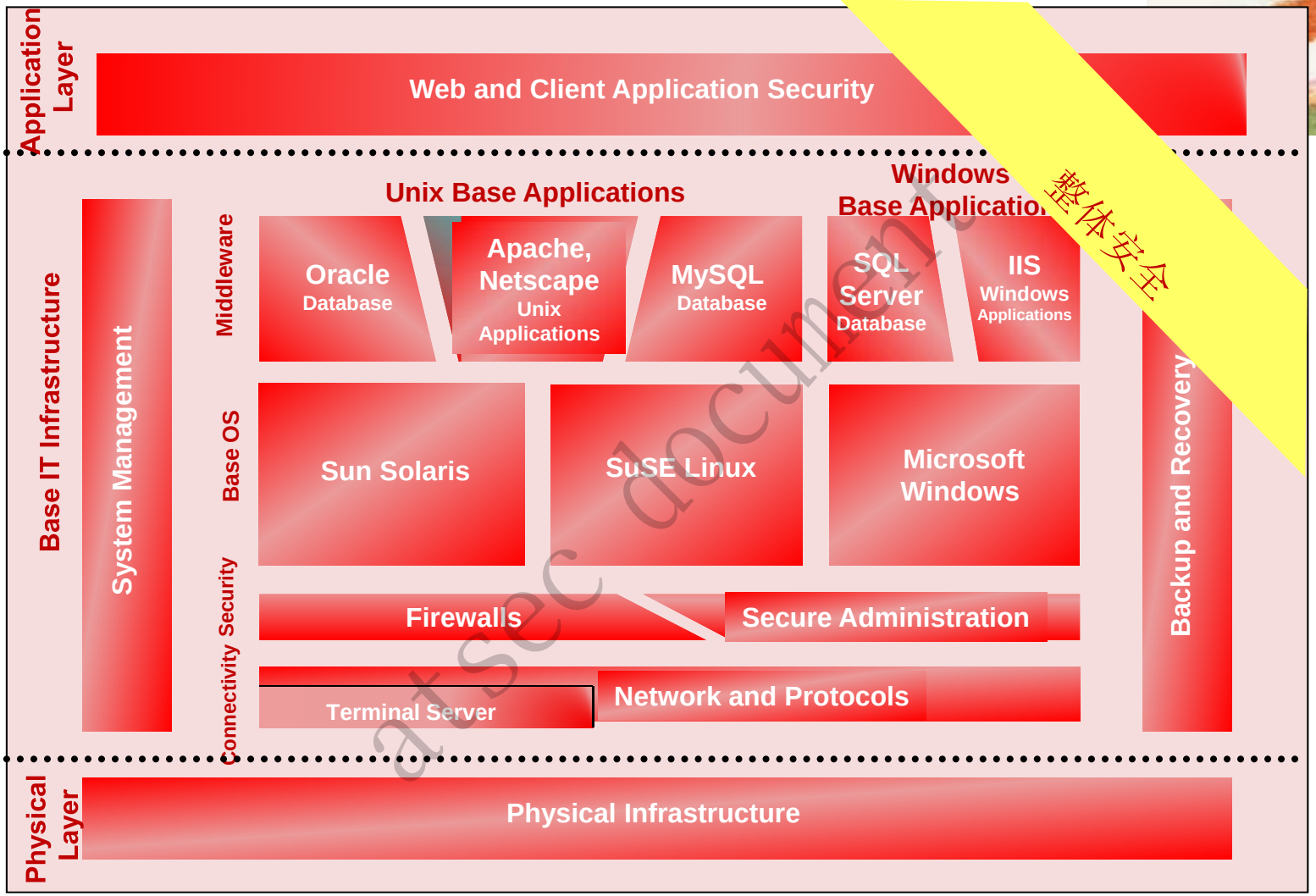
数据保护的小结

保护机制	保护后是否存有持卡人数据	业务影响	适用性描述
Masked PAN	No	高	当业务要求不需要完整卡号，且需要前六后四
Hash	No	高	当业务要求不需要完整卡号
Tokenization	No	中	当业务要求不需要完整卡号
Strong encryption	Yes	低	当需要完整卡号
Compensating control	Yes	低	当实现强加密有限制，且需要完整卡号

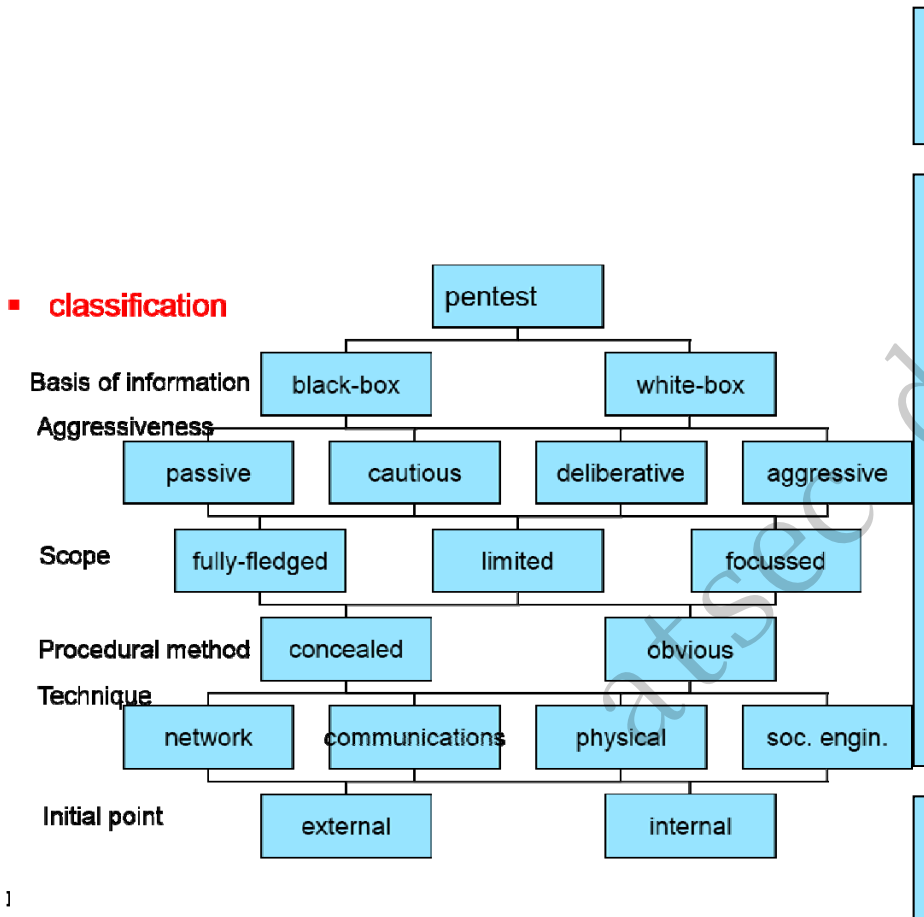
最佳实践重点分享：

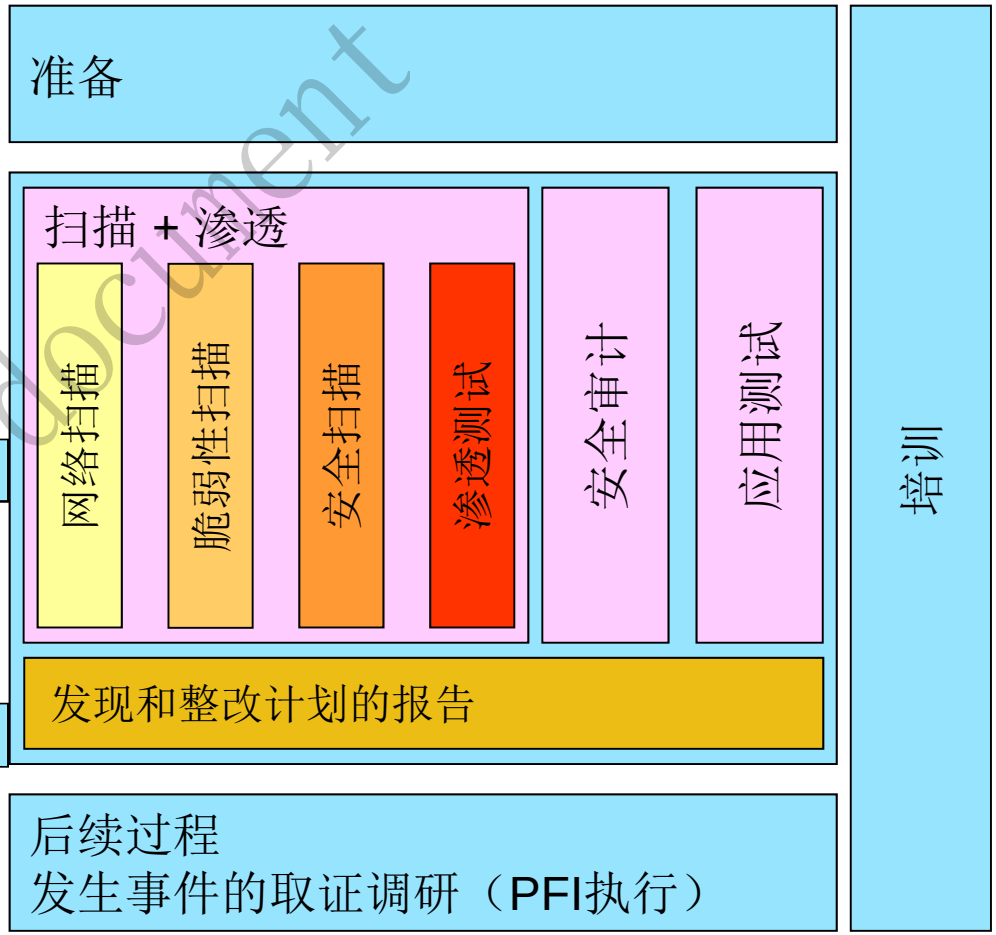
- **整合统一的信息安全管理体系**
- **密码实现**
- **合规与测试**

IT基础架构



atsec审核和测试方法论框架





Prioritized Approach

MS1: sensitive authenticatio on date and limit data

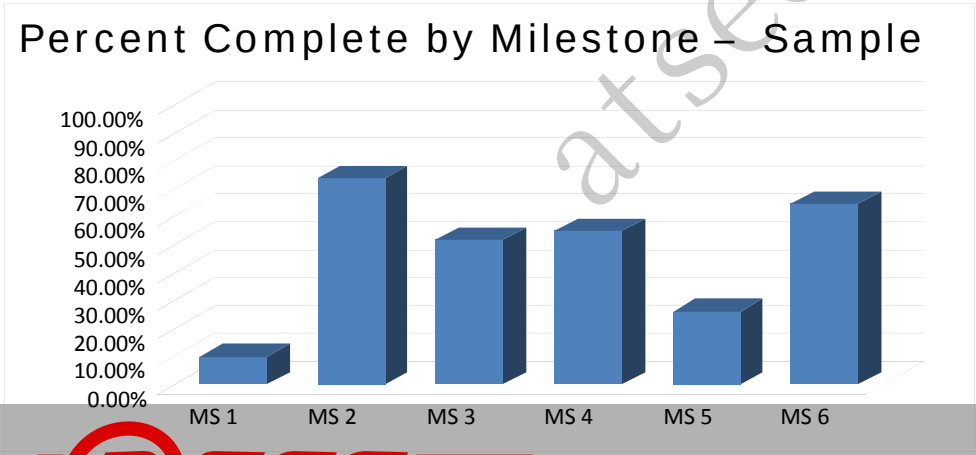
MS2: Protect the perimeter, perimeter, internal, and and wireless networks

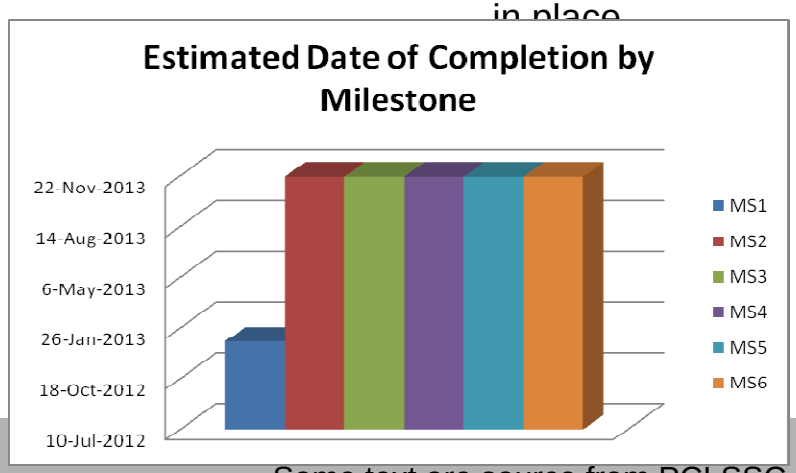
MS3: Secure payment card applications

MS4: Monitor and control access to your systems

MS5: Protect stored cardholder data

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





Some text are source from PCI SSC

安全评估中数据检查

渗透测试和诊断工具和方法
- 商业或开源工具

磁条数据可以在不同的存储位置发现

典型的违规存储位置包括？
- 数据库、文件、日志、Debug
- 纸质凭单

通常存储PAN或CVV2的系统
- POS服务器、授权服务器等

如果环境不涉及读卡器数卡或者面对面的接受数据，很可能（但不是绝对）不会涉及磁条信息。

合规状态结果查询

- 合规评估列表：
  - http://www.atsec.cn/cn/pci-compliance.html

Allinpay Network Services Co., Ltd PCI DSS v2.0	Initial Date: 2013-12-31 Issue Date: 2013-12-31 Expiry Date: 2014-12-30	atsec-2013-PCI-DSS-C-96135-0297
Amway (China) Co., Limited PA DSS v2.0	Initial Date: 2012-05-12 Issue Date: 2012-05-12 Expiry Date: 2016-10-28	Refer to SSC official website
Beijing Baidupay Science and Technology Co., Ltd PCI DSS v2.0	Initial Date: 2013-08-19 Issue Date: 2013-08-19 Expiry Date: 2014-08-18	atsec-2013-PCI-DSS-C-47271-0148
Beijing BoTongLianDa Technology Co., Ltd PCI DSS v2.0	Initial Date: 2013-07-12 Issue Date: 2013-07-12 Expiry Date: 2014-07-11	atsec-2013-PCI-DSS-C-26979-0119
Beijing Hengjiang Alliance Technology Co., Ltd PCI DSS v2.0	Initial Date: 2013-06-20 Issue Date: 2013-06-20 Expiry Date: 2014-06-19	atsec-2013-PCI-DSS-C-27941-0176
BOC Services Company Limited Kunshan branch PCI DSS v2.0	Initial Date: 2012-12-06 Issue Date: 2013-12-06 Expiry Date: 2014-12-05	atsec-2013-PCI-DSS-C-69225-0155
CHASE Science Co., Ltd PA DSS v2.0	Initial Date: 2012-07-27 Issue Date: 2012-07-27 Expiry Date: 2016-10-28	Refer to SSC official website
China CITIC Bank Corp.,Ltd. Credit Card Center PCI DSS v2.0	Initial Date: 2013-05-17 Issue Date: 2013-05-17 Expiry Date: 2014-05-16	atsec-2013-PCI-DSS-C-68210-0130
China Minsheng Bank Corp.,Ltd. Credit Card Center	Initial Date: 2012-10-15 Issue Date: 2013-10-15 Expiry Date: 2014-10-14	atsec-2013-PCI-DSS-C-74160-0125
Company Limited PCI DSS v2.0	Issue Date: 2013-12-20 Expiry Date: 2014-12-19	DSS-C-37201-0173
Shenzhen Trustspay Network Technology Co., Ltd PCI DSS v2.0	Initial Date: 2013-02-01 Issue Date: 2014-01-26 Expiry Date: 2015-01-25	atsec-2014-PCI-DSS-C-50290-0451
SHENZHEN TRUSTSWIFT ECOMMERCE CO.,LTD. PCI DSS v2.0	Initial Date: 2014-01-27 Issue Date: 2014-01-27 Expiry Date: 2015-01-26	atsec-2014-PCI-DSS-C-01316-0103
Shenzhen UnionPay Financial Network Co., Ltd. PCI DSS v2.0	Initial Date: 2014-01-29 Issue Date: 2014-01-29 Expiry Date: 2015-01-28	atsec-2014-PCI-DSS-C-06239-0307
The NET-A-PORTER GROUP China Co., Ltd PCI DSS v2.0	Initial Date: 2013-04-24 Issue Date: 2013-04-24 Expiry Date: 2014-04-23	atsec-2012-PCI-DSS-C-66228-0135
YeePay Inc. PCI DSS v2.0	Initial Date: 2010-06-03 Issue Date: 2013-09-04 Expiry Date: 2014-09-03	atsec-2013-PCI-DSS-C-36123-0502

该证书列表仅用PCI合规状态的查询，atsec保留本合规列表解释和使用的所有权利。未经atsec授权，禁止任何机构用于商业目的。关于合规和评估的具体细节，分别在每个合规报告（ROC：Report on Compliance）中进行详尽阐述。

（This compliance list is only used for PCI compliance status query, atsec retains all rights to the explanation and use of the compliance list. Any commercial purpose regarding the usage of this compliance list is explicitly prohibited except formal authorization from atsec. Compliance and assessment details are described in each individual Report on Compliance (ROC).）

通过 info_cn@atsec.com 联系atsec以获得更多PCI相关的评估和服务信息。

（Contact atsec at info_cn@atsec.com for further information on PCI related assessments and services.）

PCI DSS合规的价值

达到外部监管机构强制性要求，比如VISA、MasterCard、相关客户等；

塑造形象增强机构往来的信心

- 监管机构或者权威部门的批准；
- 客户，合作伙伴，供应商
- 机构内部组织和部门之间

进一步加强机构内部管理和控制

- 加强公司管理高级别的安全性，使高层的方针政策融入到具体的业务流程，操作流程和人事财务等行政管理流程之中，并通过工作模版/工具使得各项记录更加简化有效；
- 建立可计量的机制来获得管理支持，管理和技术使用共同语言对话；
- 在公司内增强安全控制的实务保障；
- 全员提高安全意识，全员深刻体会企业文化；
- 加强投资信心。

PCI DSS合规的价值-续

降低诸多的成本和费用

- 有效的管理和降低安全事件的影响，减小处理风险的投资，完整的风险管理，业务连续性和应急响应等细节的完善更是直接降低了重大事件发生的风险；
- 通过符合性的审计和认证，可以减少其他各个领域的外部审查或调研，比如西方客户或者法律领域经常发生的尽职调查等；
- 可以减少保险相关费用，通过符合性建设直接带来长期的必要保险费用的减低，或者保险额、保险范围的增加；
- 通过管理体系职责明确，可以与相关人员分担安全工作。
- 符合性建设和认证具有市场价值，在同行业同领域对手面前占据绝对的优势，提高自身竞争力；
- 符合性建设和认证可以为全球信息交流建立国际信任且认可的平台，是机构在世界舞台上展现自己的重要因素，也很有可能是先决条件。

全球化的视角专注于信息安全

Munich

ISO 9001
ISO/IEC 27001
ISO/IEC 17025

- Common Criteria
- Consulting
- Govt. Support
- ISMS
- *Hardware Testing*

Austin

ISO 9001
ISO/IEC 27001
ISO/IEC 17025

- Common Criteria
- CMVP
- Govt. Support
  - TWIC
  - FICAM
  - SCAP
  - NPIVP
- O-TTPS
- Consulting
- ISMS
- Hardware Testing

Stockholm

ISO 9001
ISO/IEC 27001
ISO/IEC 17025

- Common Criteria
- Consulting
- Govt. Support

Beijing

ISO 9001
ISO/IEC 27001
ISO/IEC 17025

- PCI
  - QSA
  - ASV
  - PA-QSA
  - PFI
- ISMS
- Consulting

Bangkok

- *PCI*
- ISMS
- Consulting

更多信息

- http://www.atsec.com/