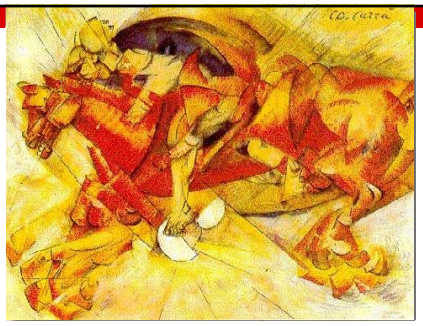
the information security provider



QUALIFIED SECURITY ASSESSOR

APPROVED SCANNING VENDOR

QUALIFIED SECURITY ASSESSOR

支付产业数据安全保护机制探讨

李迪　　资深顾问

di.li@atsec.com

内容概述

- 数据保护的范围
- 使用哈希的数据保护措施
- 使用截断的数据保护措施
- 令牌化的数据保护措施
- 强加密形式的数据保护措施
- 补偿性控制措施

PCI DSS COMPLIANT

PCI PA-DSS VALIDATED

FIPS VALIDATED 140-2

数据保护的范围

哪些数据需要保护

- **持卡人数据**
  - 卡号、持卡人姓名、过期日、服务码
- **敏感认证数据**
  - 全磁道数据、CVC2/CVV2/CID/CAV2 验证码、PIN/PIN Block 密码
- **个人信息**
  - 身份证号、地址、电话号码
- **身份验证信息**
  - 登陆密码、密码保护提示问题，个性化字符串，身份验证设备序列号、生物特征信息

产业标准强制要求保护的数据

PCI DSS V3.1

持卡人数据的存储 Storage of Card Data			
	Data Element 数据元素	**Storage Permitted 是否允许存储**	**PCI DSS 要求 3.4**
Cardholder Data 持卡人数据	Primary Account Number (PAN) 主账号	√	√
	Cardholder Name 持卡人姓名	√	☒
	Service Code 服务码	√	☒
	Expiration Date 过期日	√	☒
Sensitive Authentication Data 敏感认证数据	Full Magnetic strips 全磁道	☒	
	CVC2/CVV2/CID/CAV2 验证码	☒	
	PIN/PIN Block 密码	☒	

产业标准强制要求保护的数据

PCI DSS V3.1

允许存储敏感认证数据的特例：

用于发行信用卡卡片的情况下可以存储敏感的认证数据，但需要对该数据进行安全保护。

可能适用的机构：

- **发卡机构**
- **协助发行卡片的组织机构, 如制卡公司**

产业标准强制要求保护的数据

PA-DSS V3.1

针对密码存储的要求：

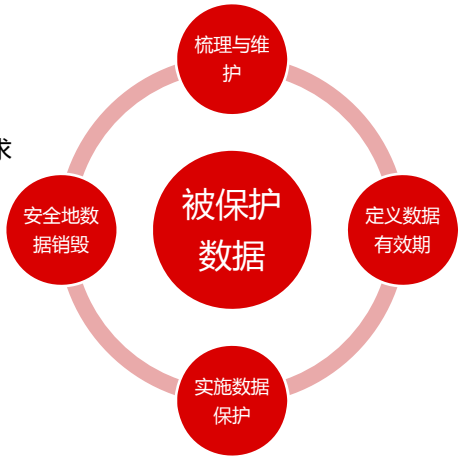
使用强效单向散列算法，基于许可标准使所有支付应用程序密码在存储期间不可读。

在应用加密算法之前，每个密码都必须组合一个唯一的输入变量。

注：输入变量不需要不可预测或加密

数据安全保护生命周期

- 数据的梳理与维护
  - 数据流向分析
  - 确定数据保存位置
- 定义数据有效期
  - 基于业务需要与外部合规要求
- 实施数据保护
  - 哈希
  - 截断
  - 令牌化
  - 强加密
  - 补偿控制措施
- 安全地数据销毁
  - 使用安全删除标准



数据保存的位置

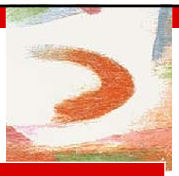
存在位置	存在形态	识别方法
数据库	数据内容	识别工具
备份介质	日志文件	人工检查
文件柜	纸张	
服务器	单据	

4	4	0	8	9	8	5	5	0	0	0	0	0	5	8	5
x2		x2		x2		x2		x2		x2		x2		x2	
8		0		18		10		0		0		0		16	
				-9		-9								-9	
8	4	0	8	9	8	1	5	0	0	0	0	0	5	7	5

Regular Expression Searches for Credit Card Numbers

Visa: ^4[0-9]{12}(?:[0-9]{3})?$ - All Visa cards start with a 4.
MasterCard: ^5[1-5][0-9]{14}$ - All MasterCard start with the numbers 51 through 55.
American Express: ^3[47][0-9]{13}$ - American Express cards start with 34 or 37.
Diners Club: ^3(?:0[0-5]|[68][0-9])[0-9]{11}$ Diners Club cards begin with 300 through 305, 36 or 38.
Discover: ^6(?:011|5[0-9]{2})[0-9]{12}$ Discover card numbers begin with 6011 or 65.
JCB: ^(?:2131|1800|35\d{3})\d{11}$ JCB cards beginning with 2131 or 1800 have 15 digits.
JCB cards beginning with 35 have 16 digits.

atsec数据检测方案价值



检测方案价值	检测方案的特性
简化机密数据的定义与识别	• 支持多达95种机密数据识别。 • 可检测持卡人数据、个人信息、财务信息等多类数据。
助力合规建设	• 有效支持达到PCI DSS，HIPAA等多个标准合规管理。
消除支付产业合规的难点	• 可支持邮件应用系统、数据库应用系统、大型机系统的数据检测
降低合规管理成本	• 定制化的数据检测任务 • 自动化的数据检测报告

atsec数据检测方案功能说明

- 检测范围
  - 支付数据
  - 个人信息
  - 财务数据
- 检测能力
  - 内存空间
  - 邮件系统
  - 数据库系统
  - 影像与传真
  - 云端APP
- 检测管理
  - 跨平台支持
  - 定制化报告

数据存储示例

所属机构	所属部门	所属应用或业务	系统(IP)	文件或表	信用卡数据	保护机制	访问日志	存储原因	存储有效期
XXX结算公司	收单部	MAS商户收单服务	应用服务器（10.1.2.34）	文件：D:\business\Data*	PAN, Name, Expiration	截断	DB2数据库访问日志	收单业务使用	3年
	收单部	MAS商户收单服务	数据库服务器（10.9.10.3）	表：CAM_Hwerwd	PAN, Name, Expiration	软加密	交易日志	收单业务使用	2年
	收单部	MAS商户收单服务	数据库服务器（10.1.1.34）	日志：onltranrechis,posonltranrechis,bsmonltranrechis	PAN	软加密	无	收单业务使用	1年

常见的数据保护机制1 – 哈希

保护机制1：哈希

- 什么是哈希
  - 又称单向散列函数，把数据压缩成固定长度的摘要，使得数据量变小
  - 如果两个散列值是不相同的（根据同一函数），那么这两个散列值的原始输入也是不相同的
  - 散列函数具有不可逆性
  - 可能发生的问题：哈希碰撞
- 为什么使用哈希
  - 代替原始数据存储
  - 存储数据只用于比对，不能从存储数据还原成原始数据

哈希算法及其使用

- 哈希算法
  - SHA-2家族
    - SHA-224、SHA-256 、SHA-384、SHA-512
  - SHA-3家族
    - SHA3-224、SHA3-256 、SHA3-384、SHA3-512
- 使用方式
  - result = HashFunction (input)
  - result = HashFunction (input + salt)
  - “1111222233334444”，计算SHA-256: result=c6b25ffac5d2c50f41af3ac4d97d07d95fd4f2d5f9fcef98dc709e5741060508

常见的数据保护机制2 – 截断

保护机制2: 截断

类别	截断	哈希
形式	439234xxxxxx1234	729129118523184663129
业务需要	需要验证卡BIN	需要验证是之前的某张卡号
适用场景	显示在业务日志中用于查错 显示于界面中用于用户验证	仅需确认是某张已使用卡号

- 为什么使用截断
  - 代替原始数据存储
  - 存储数据只用于比对，不能从存储数据还原成原始数据
  - 不能和哈希结果存储在一起

对同时使用截断和哈希的额外要求

前提	• 使用截断和哈希进行相同卡号的保护
形式	• 加密、访问控制等
原因	• 降低重建原始数据的风险

PCI DSS Requirement 3.4 注：对恶意个人而言，如果能访问被截词和散列的PAN，要重建原始PAN数据是件相当轻松的事。如果在实体环境中出现同一个PAN的散列版本和截词版本，则应采取额外控制措施，确保散列版本和截词版本不能被相互关联，用于重建原始PAN。

保护机制2: 截断

- 显示 PAN 时对其进行掩盖（最佳的做法是只显示的数位包括前六位与后四位，仅在业务需要时可以查看完整的卡号信息）。
- 参见VISA发布的文档《Visa Best Practices for Primary Account Number Storage and Truncation》
- Example: 412345XXXXXX6789 or XXXXXXXXXXXX1234 for the PAN and XXXX for the expiration date.

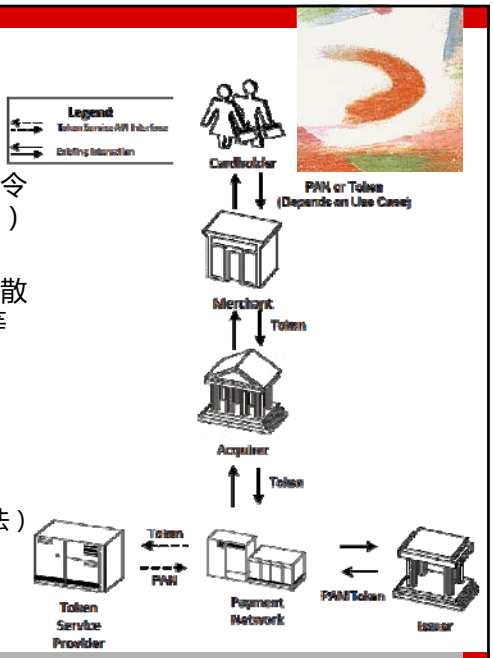
常见的数据保护机制3 – 令牌化

保护机制3: 令牌化

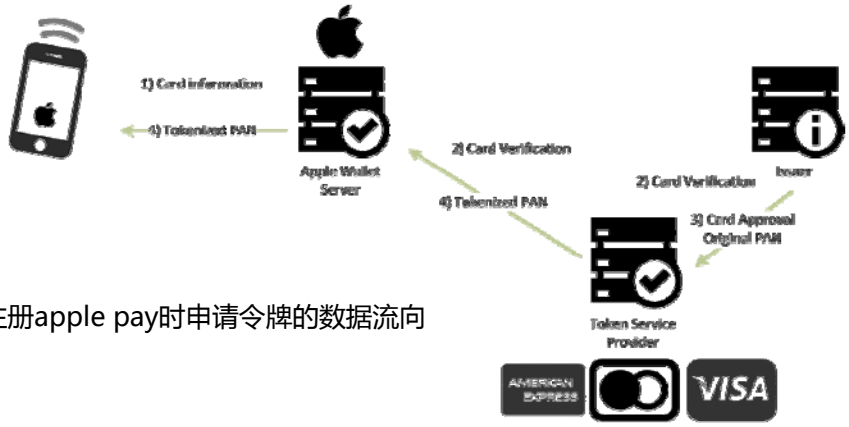
- 令牌化指在交易中用一个替代值（令牌）来替换高价值的认证码（卡号）的过程。
- 令牌化可以采取多种方案，如单向散列、截断+序列号、EMVCo方案等

- EMVCo定义的令牌需要符合：
  - 13~19位数字
  - 专属的卡BIN范围
  - 符合基本的卡号验证规则（Luhn算法）
  - 不能和实际卡号冲突

EMVCo Payment Tokenisation Specification Technical Framework



保护机制3: 令牌化



- 注册apple pay时申请令牌的数据流向

保护机制3: 令牌化

- 使用apple pay 进行近场刷卡交易（NFC）时的数据流向

保护机制3: 令牌化

- **Apple wallet 界面展示**

常见的数据保护机制4 – 强加密

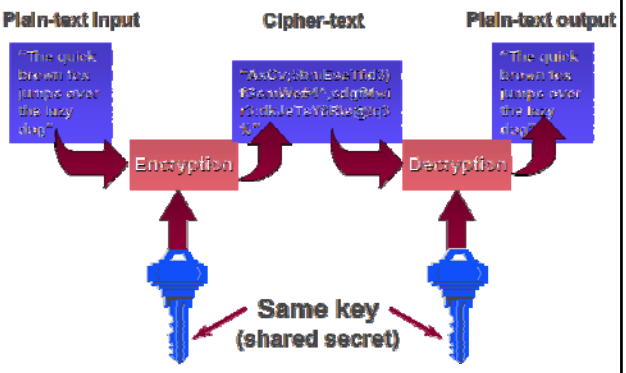
保护机制4: 强加密

- 加密算法的选择
  - 不要使用私有的加密算法
  - 使用业界认可的算法
    - NIST FIPS 140-2
    - 商密
  - 对称加密算法 VS 非对称加密算法
- 加密算法的实现
  - 尽量不要使用自研的加密算法库
  - 使用公开的加密算法库
    - MS DPAPI，JAVA CAPI，OpenSSL

对称加密算法

- 加解密密钥相同
- 加密解密双方都需要对密钥进行保护
- 计算速度快
- 适合加密长数据

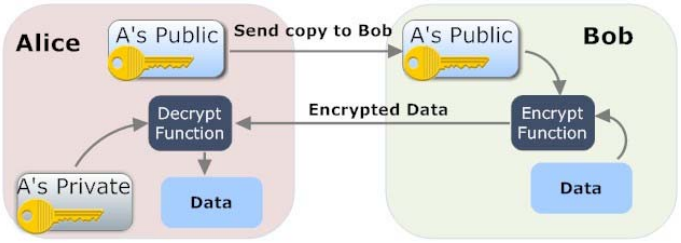
- 常用算法：
  - 3key TDES
  - AES
  - SM4



非对称加密算法

- 加密解密密钥不同，分为公钥和私钥，两者是唯一的一对
- 公钥可以公开，私钥需要保密
- 计算速度慢
- 适合对小数据进行加密

- 常用算法：
  - RSA 2048
  - ECDSA 256
  - SM2



加密算法强度

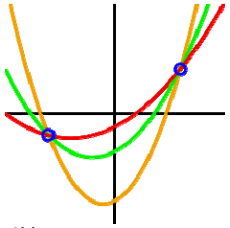
安全位数Bits of security	对称密钥算法 Symmetric key algorithms	IFC (RSA)	ECC (ECDSA)
80	2key TDES	k = 1024	f = 160-223
112	3key TDES	k = 2048	f = 224-255
128	AES-128	k = 3072	f = 256-383
192	AES-192	k = 7680	f = 384-511
256	AES-256	k = 15360	f = 512+

思考：使用RSA2048来保护AES128是否可行？

密钥管理体系

知识分离机制

- 知识分离机制通常被用作管理主密钥（根密钥）
- 知识分离意味着使用密钥组件
  - 不能直接将主密钥拆分成几个组件
  - 可采用**Shamir's Secret Sharing**方案
  - 任何一个人不能获得重建密钥所需的所有部分



- 假设主密钥 S=1234
- 期望分散成6部分，任意3部分组合在一起通过计算都可以恢复出原始密钥
- D_0=(1, 1494)，D_1=(2, 1942)，D_2=(3, 2578)
- D_3=(4, 3402)，D_4=(5, 4414)，D_5=(6, 5614)

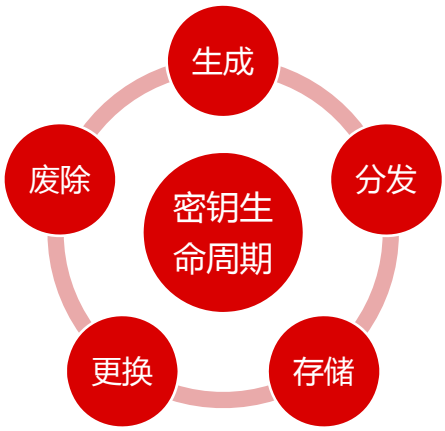
基于密码的密钥生成机制

- 密钥长度太长，不可能记得住
  - 8位密码：23190877
  - 256bit密钥：
    523d904c8f2df96634d9eed3b444838ef5f8b30c7
    059292405a5dfe5acf33855
- PBKDF2 (Password-Based Key Derivation Function)
  - 输入密码，盐值，迭代次数，密钥长度
  - 输出指定长度的密钥
    - 密码：123456；盐值：654321；迭代：1000次； 长度256bits
    - 输出：
      523d904c8f2df96634d9eed3b444838ef5f8b30c7059
      292405a5dfe5acf33855

常见的密钥时用错误

- 一个密钥多处使用
- 密钥明文写在代码中
  - 常见情况：主密钥或加密密钥写死在代码中
- 使用加密手段对密码进行保护
  - PA-DSS 要求3.3.2: 使用基于批准标准的强壮、单向加密算法使所存储的支付应用密码不可读。在应用加密算法前，每个密码必须使用与之关联的唯一的输入变量。
    Use a strong, one-way cryptographic algorithm, based on approved standards to render all payment application passwords unreadable during storage. Each password must have a unique input variable that is concatenated with the password before the cryptographic algorithm is applied。

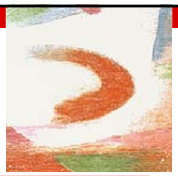
密钥管理流程



思考：
如何定义每个密钥的有效期？
NIST SP800-57

如何在密钥替换时保证业务的高可用性？

密钥更换周期



密钥类型Key Type	密钥周期Cryptoperiod	
	发起方使用周期 Originator-Usage Period	接收方使用周期 Recipient-Usage Period
1. 签名生成私钥Private Signature Key	1至3年	–
2. 签名验证公钥Public Signature-Verification Key	多年使用(取决于密钥长度)	
3. 对称认证密钥Symmetric Authentication Key	≤2 年	≤OUP + 3 年
4. 认证私钥Private Authentication Key	1 至2年	
5. 认证公钥Public Authentication Key	1 至 2年	
6. 对称数据加密密钥Symmetric Data Encryption Keys	≤2 年	≤OUP + 3 年
7. 对称密钥包裹密钥Symmetric Key Wrapping Key	≤2 年	≤OUP + 3 年
8. 对称随机数生成密钥Symmetric RBG Keys	见 SP800-90	–
9. 对称主密钥Symmetric Master Key	大约1年	–

密钥更换周期

10. 密钥传输私钥Private Key Transport Key	≤2 年
11. 密钥传输公钥Public Key Transport Key	1 到 2年
12.对称密钥协商密钥Symmetric Key Agreement Key	1 到 2年
13. 密钥协商私钥Private Static Key Agreement Key	1 到 2年
14. 密钥协商公钥Public Static Key Agreement Key	1 到 2年
15. 密钥协商临时私钥Private Ephemeral Key Agreement Key	一次密钥协商周期
16. 密钥协商临时公钥Public Ephemeral Key Agreement Key	一次密钥协商周期
17. 对称授权密钥Symmetric Authorization Key	≤2 年
18. 授权私钥Private Authorization Key	≤2 年
19. 授权公钥Public Authorization Key	≤2 年

常见的加密实现方案

方案名称	典型方案	投资成本	适用场景
硬件加密机	1、国产SJWxx加密机 2、Safenet Luna	硬件成本：高 维护成本：低	异构(或MSSQL和Oracle外)的数据库系统； 对加密性能有较高要求
数据库加密软件	Oracle TDE MSSQL TDE	软件成本：高 维护成本：低	仅Oracle或MSSQL数据库系统
自开发应用	自开发加密实现	软件成本：高 维护成本：中	所有场景
文件/磁盘加密方案	VeraCrypt, Bitlocker等	软件成本：中 维护成本：低	仅适用于加密磁盘/文件的场景

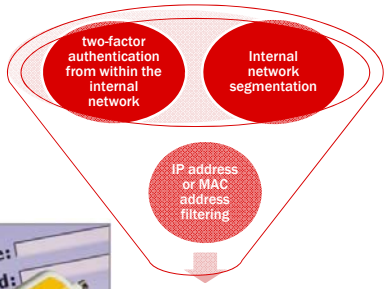
常见的数据保护机制5 – 补偿控制

保护机制5: 可参考的补偿控制措施

- 如果系统中的数据加密由于限制无法实现。比如金融机构的持卡人数据环境因性能原因暂时不能实现加密。

- 可以考虑的补偿控制如下（同时满足）：
  - (1) 内部网络分隔;
  - (2) IP地址或MAC地址过滤；
  - **(3) 内部网络实施双因素控制**

- 注意：补偿控制需要定期审核



补偿控制

小结

具体保护措施的选择策略

保护机制	业务影响	典型的实施位置	选择场景
截断或哈希	*****	业务操作界面显示、支付应用日志	当业务要求不需要完整的卡号，或者仅需要前六后四。
令牌化处理	***	组织内部不同的数据交互过程中	当业务处理需要验证卡号的唯一性，但不需要看到完整卡号。
强加密处理	**	核心数据库的存储	当需要保存和使用完整的卡号信息时。
环境的补偿控制手段	*	运维或业务操作人员的访问入口	无法实施上述三种措施且需要使用完整的持卡人数据时。

谢谢!

www.atsec.cn