小微金服密钥管理规范

文档控制

拟　制	若昭
审核	聊闲，仙剑
读　者	小微金服密钥管理和操作人员、密钥使用需求方

修订历史

版本号	作者	内容提要	拟定日期
0.1	肖淑婷（若昭）	拟定	2014-7-18
0.2	肖淑婷（若昭）	补充 PCI DSS 规范对信用卡相关业务的密钥安全管理要求；定义小微业务密钥分类和密钥周期。	2014-8-4

目录

目录

第一章总则

第一条　为确保小微金服密钥安全管理，规范密钥生成、存储、分发、算法和密钥长度、密钥周期及更新，满足业务所需的安全服务。

第二条　小微金服使用密码算法和密钥的所有业务场景均遵从本规范，本规范自发布之日起施行。

第三条　本规范由小微金服-CRO-系统安全部制定。

第二章术语和名词定义

第四条　密码技术基本概念：

密码算法指经过精心定义的一个计算过程，接受若干个输入（包括密钥），然后生成一个输出。**密钥**是密码算法使用的一个参数，知道这个参数就可以进行正向或反向的密码运算，反之不能。**密钥长度**指以 bit 为单位计数的密钥长度。**安全强度**指破解密码算法需要的工作量，通常用 bits 表示，英文常用 Security Strength 或 Bits of Security 表示。

第五条　密码算法可分为加密、数字签名、Hash 函数、消息认证码(MAC) 四类：

加密指使用密码算法和密钥将明文转换为密文的过程。加密算法有对称加密和非对称加密算法两类。**数字签名**是对数据进行密码运算转换，在恰当的基础设施和策略下，可提供源认证、数据完整性和抗否认这三项安全服务。**Hash 函数**是一种将任意长度数据转换为固定长度数据的函数，设计良好的 hash 函数具有单向性和抗碰撞性(单向性：要找到匹配一个指定输出的输入数据在计算上不可行；抗碰撞：要找到能够产生相同输出的不同输入数据在计算上不可行。**消息认证码**(Message Authentication Code, MAC)基于数据和密钥产生定长值作为认证符，数据接收方用相同的算法和密钥对接收到的数据进行计算并与接收到的认证符比较；常用的消息认证码计算方法有

基于 DES 和基于 hash 函数的。

第六条　密钥周期规定密钥可用的时间段，基于指定期限和/或密文生成的数量等。

第七条　本规范中提及的密码算法名称及缩写：

TDES：“三重数据加密标准(Triple Data Encryption Algorithm)”的缩写，也称为“TDEA”、“3DES”或“三重 DES”。

2TDEA：双倍长密钥的3DES算法，Two-key Triple Data Encryption Algorithm

3TDEA：三倍长密钥的3DES算法，Three-key Triple Data Encryption Algorithm

AES：高级加密标准，Advanced Encryption Standard，[FIPS197]

RSA：一种非对称算法，基于大数素因子分解难题，可用于进行非对称加密和数字签名。

DSA：数字签名算法（Digital Signature Algorithm），由 NIST 于 1991 年提出，用于数字签名标准（Digital Signature Standard, [FIPS 186] ）。建立在求离散对数的困难性上，仅能用于数字签名。

ECC：Elliptic Curves Cryptography，椭圆曲线算法

D-H：Diffie-Hellman 密钥交换算法

第八条　安全服务定义：

数据机密性——保证信息不被非授权泄露。

数据完整性——保证数据不被未授权的实体篡改。

认证——保证通信的实体是它所声称的实体。

授权——控制谁能存取、在什么条件下可以存取资源，可以将存取的资源用于做什么。

抗否认性——防止发送方发送过某条消息。

第三章密钥生成

第九条　非对称密钥私钥应由小微金服密钥管理部门（系统安全部）生成。

第十条　对称密钥可由参与密码运算的任意一方所在机构的密钥管理部门生成，并以安全的方式分发到对方机构的密钥管理部门。

第十一条　密钥应以不可预测的方式生成，操作时采用小微金服密钥管理基础设施（KMI）生成密钥。

第十二条　密钥数据必须严格遵循生产环境和研发环境数据隔离的要求。

第四章密钥存储

第十三条　对密钥存储的安全要求有：

(一) 私钥、对称密钥内容绝对禁止以明文形式出现在永久存储介质中；

(二) 密钥须加密存储于磁盘等永久介质中，加密算法应足够强壮，加密密钥须是安全管理的。如下两种方式管理的密钥被认为是安全的：

i. 使用硬件安全模块加密保护;

ii. 多人掌握分量且分量有严格的访问控制和授权机制。

(三) 对于一般的密钥，密钥内容可在内存等非持久存储介质中以明文形式出现和参与运算，但根据国家政策、行业规范、经公司评估安全要求特别高，必须使用硬件安全模块保护密钥和进行加解密运算的，密钥明文不能出现在硬件安全模块之外。

第五章密钥分发、传输

第十四条　因工作需要，要从线上密钥管理系统中导出签名私钥、对称密钥内容明文内容的，须经业务需求方提交需求，系统安全部密钥管理员评估需求，评估需求合理后，再由业务方和系统安全部主管审批，审批通过后再由密钥操作员执行。

合理的密钥导出需求有：以离线方式分发对称密钥到已确认的合作机构。对于非合理的密钥导出需求，密钥管理员应在评估阶段拒绝。

第十五条　密钥加密密钥须以安全的方式分发。

密钥在网络中传输须加密，加密算法和密钥强度不小于密钥本身对应的算法和强度。

用口令加密方式传输密钥时，密钥密文和口令采用不同的通讯方式传输。

通过密钥管理专员以线下方式分发时，须确保密钥介质的物理安全性。

第六章密码算法和密钥强度规范

第十六条　在选择密码算和密钥长度时，遵循下述原则：

(一) 应根据业务所需的安全服务来选择恰当的密码算法：

可提供机密性保护的密码算法有：对称加密算法（3DES、AES）和非对称加密算法（RSA、ECC）。

可提供完整性保护的密码算法有：消息认证码（MAC）、数字签名算法（RSA、DSA、ECDSA）和Hash算法。

可提供消息来源认证的密码算法有：消息认证码（MAC）和数字签名算法（如：RSA、DSA、ECDSA）。

可提供抗否认性的密码算法有数字签名算法（如：RSA、DSA、ECDSA）。

(二) 应根据业务所需的安全强度、对数据的保护时间跨度要求选择恰当的密钥长度:

表2 推荐的安全强度标准（NIST SP800-57）

安全强度		**2011年~2013年**	**2014~2030年**	**2031年之后**
80	应用	不推荐	不允许	不允许
	处理	遗留使用		
112	应用	可接受	可接受	不允许
	处理			遗留使用

128	应用/处理	可接受	可接受	可接受
192		可接受	可接受	可接受
256		可接受	可接受	可接受

注：本表中，” 应用”指将密钥用于新数据，如加密、计算签名；“处理”对已经密码算法保护的数据进行处理，例如解密、验证签名。

表3 密码算法和HASH算法的安全强度 （NIST SP800-57）

安全强度 (Bits of Security)	**对称密钥算法**	**DSA, D-H**	**RSA**	**ECC**	**Hash:数字签名和纯hash应用**	**HMAC**
80	2TDEA	L=1024 N=160	k=1024	f=160~223	SHA-1及以上	SHA-1及以上
112	3TDEA	L=2048 N=224	k=2048	f=224~255	SHA-224及以上	SHA-1及以上
128	AES-128	L=3072 N=256	k=3072	f=256~383	SHA-256及以上	SHA-1及以上
192	AES-192	L=7680 N=384	K=7680	f=384~511	SHA-384及以上	SHA-224及以上
256	AES-256	L=15360 N=512	K=15360	f=512+	SHA-512	SHA-256及以上

(三) 特别地，涉及信用卡数据处理的相关业务，应遵照PCI-DSS的要求采用强效加密法，加密算法和密钥长度须符合PCI-DSS最新版本中“强效加密” 的定义。本规范制定时，PCI-DSS最新版本为3.0,2014年1月发布，其中对“强效加密”的定义为：“以经过行业测试和认可

的算法为基础的加密法，密钥长度较长（至少 112 位的有效密钥长度）且密钥管理方法合适。加密法是一种保护数据的方法，包括加密（可逆的）和散列（不可逆的或单向的）。本文发表时，就最小加密强度而言，经过行业测试和认可的标准和算法包括 AES（128 位和更高）、TDES（最少三倍长的密钥）、RSA（2048 位和更高）、ECC（160 位和更高）以及 ElGamal（2048 位和更高）。"

第七章密钥周期与更新

第十七条 应对每一个密钥定义使用周期，允许采用两种定义方式：

(一) 所保护的数据达到一定量

(二) 密钥使用时间达到一定期限

第十八条 在设定密钥周期具体量值时，应综合考虑密码算法所保护处理过程的重要性、密钥被泄露后的不良影响程度、密钥泄露的风险大小。

密钥泄露的风险因素有：密码算法的安全性、密钥强度、操作环境的安全性、所保护数据的存活时间、密钥的存储份数和分发方式。

表 4 小微业务密钥的推荐密钥周期

密钥分类	**按用途细化分类**	**密钥周期**
签名密钥	支付宝系统之间对业务数据进行签名	2 年
	支付宝与阿里集团 BU 之间对业务数据签名	2 年
	支付宝与外部机构之间业务签名	2 年
	证书（网站证书、企业签名证书）	1 年
加密密钥	支付宝系统存储敏感信息加密	2 年
	支付宝系统间传输敏感信息加密	2 年
	支付宝与阿里集团 BU 之间传输业务数据加密	2 年

	支付宝与外部机构之间传输业务数据加密	2 年
认证密钥	支付宝系统存储密码类数据时的 hash-salt	2 年
	支付宝系统之间传输业务数据时的消息认证密钥	2 年
	支付宝与阿里集团 BU 之间传输业务数据时的消息认证密钥	2 年
	支付宝与外部机构之间传输业务数据时的消息认证密钥	2 年
认证密码	数据库访问密码	2 年
	支付宝内部服务访问密码	2 年
	外部服务访问用户名密码	2 年

第十九条　按 PCI DSS 要求，信用卡数据加密密钥周期为 1 年。

第二十条　在符合下面三个条件之一时应进行密钥内容更新，相关业务需在风险评估确定的期限内切换到新密钥：

(一) 对密钥的使用达到密钥周期上限；

(二) 已确定密钥被泄露或疑似泄露；

(三) 知道密钥明文的人员离职或转岗。